Kurzgutachten I.S.S. Schulmensaverwaltung

1 Zusammenfassung

Mit diesem Gutachten werden die Ergebnisse der datenschutzrechtlichen und IT-sicherheitstechnischen Prüfung der Anwendung I.S.S. Schulmensaverwaltung, bestehend aus den Modulen I.S.S. Webportal, I.S.S. Debitorenverwaltung und I.S.S. POS sowie der Schnittstelle zum I.S.S. Service-Center dokumentiert, mit der die intersoft consulting services AG seitens der People & Projects IT GmbH beauftragt wurde. Nicht Teil der Begutachtung ist das Fingerprintverfahren sowie das RFID-Verfahren, mit welchen die Identifizierung am I.S.S. Terminal (innerhalb des I.S.S. POS) stattfindet.

I.S.S. Schulmensaverwaltung ist eine multifunktionale Anwendung zur Unterstützung von Schulen bei der Verwaltung der Mensa. Es ist sowohl bei öffentlichen Stellen (den Schulen) als auch in der Privatwirtschaft (den von den Schulen beauftragten Caterern) einsetzbar.

Hersteller ist die in Elmshorn ansässige People & Projects IT GmbH, welche die Anwendung selbst erstellt hat und fortlaufend entwickelt. Die Anwendung bietet neben den Erleichterungen in der Verwaltung der Mensa für Schulen und Caterer vor allem den Teilnehmern am Schulmensaessen ein unkompliziertes webbasiertes Verfahren, um sich an- und abzumelden und die Bezahlung vorzunehmen. Insofern handelt es sich bei dem auditierten Gegenstand sowohl um ein IT-Produkt als auch um einen IT-basierenden Service. Innerhalb des Moduls I.S.S. POS gehören die Verfahren RFID und Fingerabdruck nicht zum Zertifizierungsgegenstand.

Die Prüfung wurde anhand der Kriterien des Datenschutz-Gütesiegels gemäß der Schleswig-Holsteinischen Landesverordnung über ein Datenschutzaudit (DSAVO) [1] durchgeführt. Grundlage für die Erstellung dieses Gutachtens gemäß DSAVO ist die Version 1.2 des Anforderungskatalogs für ein Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein (ULD).

Im Ergebnis stellt der Auditor fest, dass die I.S.S. Schulmensaverwaltung unter Beachtung der dem Anwender zur Verfügung gestellten Datenschutzhinweise konform zu den gesetzlichen Anforderung an den Datenschutz und die IT-Sicherheit ist und den Datenschutz fördert.

A – Allgemeiner Teil

1 Zeitraum der Prüfung

Die Auditierung von I.S.S. Schulmensaverwaltung erstreckte sich auf den Zeitraum vom 09. Juli 2012 bis 28. Juni 2013 und beinhaltete eine strukturierte Datenschutzanalyse auf der Basis von Interviews, der Durchführung von Tests, der Sichtung von Dokumentationen sowie Besichtigungen vor Ort.

---

[1] Landesverordnung über ein Datenschutzaudit (Datenschutzauditverordnung - DSAVO) *vom 18. November 2009 Fundstelle: GVOBl. 2008, S. 562 / GVOBl. 2009, S. 742*

2 Antragstellerin

Antragstellerin der Auditierung und Zertifizierung gemäß DSAVO ist die

People & Projects IT GmbH
Daimlerstraße 17
25337 Elmshorn
(im folgenden PPIT)

als Hersteller des IT-Produkts I.S.S. Schulmensaverwaltung und als IT-Dienstleister.

Ansprechpartner ist Herr Thomas Abel, Geschäftsführer der People & Projects IT GmbH.

3 Sachverständige Prüfstelle

Sachverständige Prüfstelle gemäß DSAVO ist die

intersoft consulting services AG
Frankenstr. 18a
20097 Hamburg
Tel.: 040 79 02 35 – 0
E-Mail: info@intersoft-consulting.de
Web: www.intersoft-consulting.de

unter der Leitung von Herrn Matthias Lindner (Recht/Technik).

4 Kurzbezeichnung des IT-Produktes/IT-Services

Auditiert wurde das Produkt I.S.S. Schulmensaverwaltung, bestehend aus den Modulen I.S.S. Webportal, I.S.S. Debitorenverwaltung und I.S.S. POS sowie der Schnittstelle zum Service-Center in der Version 1.0 sowie der entsprechende IT-basierende Service.
Fingerprintverfahren und RFID-Verfahren gehören nicht zum Zertifizierungsgegenstand.

Der E-Mail-Support des Service Centers (hier wird Exchange SaaS eingesetzt) gehört nicht zum Zertifizierungsgegenstand, der Support des Service-Centers erfolgt hier nur telefonisch.
Es wird darauf hingewiesen, dass die türkischen Sprachversionen der Erklärungen im I.S.S. Webportal nicht von den Sachverständigen überprüft wurden.
Zudem sind Aktionen und Umfragen, welche in den AGB Erwähnung finden, nicht Teil der Zertifizierung.
Bestellungen per App, SMS und Email gehören ebenfalls nicht zum Zertifizierungsgegenstand.

5 Detaillierte Beschreibung des IT-Produkts/IT-Services

5.1 Zweck

Im Rahmen des I.S.S. Webportals der I.S.S. Schulmensaverwaltung können Anmeldungen und/oder Abmeldungen zum Schulmensaessen durchgeführt werden. Zudem werden über dieses Portal die Abrechnung der Essensteilnahme sowie der Zahlungsverkehr vorgenommen und abgewickelt.

Arten der Bezahlung können Selbstzahler (Vorkasse) und Nutzung des Bankeinzugsverfahren sein. Die Beschreibung und der Umgang mit der Bezahlung ist in den AGB's hinterlegt[2].
Wird der Mindestbetrag erreicht, wird über die I.S.S. Debitorenverwaltung eine DTAUS Datei erzeugt. Diese DTAUS-Datei wird in das genannte Treuhandkonto importiert. Zur Datenimportierung nutzt PPIT die banküblichen Programme (Volksbank: VR-Networld) Die Zuordnung der Beträge erfolgt über die Teilnehmernummer im Sammellastschriftverfahren.
Zahlungseingänge der Selbstzahler werden manuell dem Guthabenkonto des Teilnehmers zugeordnet und gebucht. Teilnehmer können den Zahlungseingang innerhalb des I.S.S. Webportals überprüfen.

Die Nutzung der I.S.S. Schulmensaverwaltung setzt eine Anmeldung zum System voraus. Das Anmeldeformular kann über die Startseite der jeweiligen Schulwebsite unter „Registrierung" abgerufen werden. Es erfolgt anschließend eine Aufforderung zur Eingabe der persönlichen Daten, wobei Pflichtfelder durch ein „*" gekennzeichnet sind. Das System führt den Teilnehmer durch die Anmeldung.
Die Passworteinstellungen werden zum neuen Schuljahr so geändert, dass der Nutzer sofort nach dem ersten Login zum Passwortwechsel aufgefordert wird.
Die Erhebung der Daten erfolgt auf freiwilliger Basis. Das System der PPIT greift nicht auf den Server einer Schule zurück.

Die Komponenten „Verwaltung" und „Debitor" werden in der Dokumentation zu „Debitorenverwaltung" zusammengefasst.
Die Komponenten „Terminal Essensausgabe" und „Terminal Kioskbetrieb" sind als POS zu interpretieren. Alle Komponenten werden von PPIT betrieben.

Der Service-Center ist eine telefonische Anlaufstelle für die Anwender. Schulmensaverwaltung und Service-Center werden von PPIT betrieben.

5.2 Einsatzbereich

Das IT-Produkt soll für den Einsatz in Schulmensen verwendet werden und ist daher für den Einsatz bei öffentlichen Stellen des Landes Schleswig-Holstein geeignet.

6 Modellierung des Datenflusses

Mit I.S.S. Schulmensaverwaltung werden sowohl Primär- als auch Sekundärdaten erhoben und verarbeitet.

6.1 Primärdaten

Nr.	Datenart	Personengruppe	Datenfelder
1	Stammdaten Mensaesser	Schüler Lehrer = Mensaesser	Vorname Nachname Schule Klasse Geschlecht

[2] Siehe Anlage 10, AGB, § 4, Seite 20.

			Teilhabeleistung regelmäßige Essenstage Foto
2	Essensdaten	Mensaesser	Tag Essensnummer
3	Gesundheitsdaten	Mensaesser	Allergene Besonderheiten
4	Stammdaten Essenszahler	Eltern von Schülern Lehrer = Essenszahler	Anrede Vorname Nachname Erziehungsberechtigung Straße und Hausnummer PLZ und Wohnort Telefonnummer E-Mail Adresse
6	Zahlungsdaten	Essenszahler	Bankverbindung Guthabenstand

6.2 Sekundärdaten

7	Protokolldaten Essenszahler	Essenszahler	An- und Abmeldedaten Schreibende Datenbankzugriffe
8	Protokolldaten Admin	Mitarbeiter People & Projects IT GmbH	An- und Abmeldedaten Schreibende Datenbankzugriffe

6.3 Beschreibung der Datenarten

6.3.1 Primärdaten

Pflichtfelder sind:

- Angabe, ob man Elternteil, Schüler/in oder Verwaltungsmitarbeiter/in ist
- Welche Schule besucht wird
- Für welches Schuljahr die Anmeldung erfolgt
- Klasse des Kindes
- Vorname und Nachname des Kindes
- Geschlecht des Kindes
- Angabe, ob Anmeldender oder das Kind Leistungen aus dem Bildungspaket oder andere Förderleistungen z.B. für das Mittagessen erhält
- Angaben zu der anmeldenden Person:
- Vorname und Nachname

- Straße und Hausnummer, Postleitzahl und Wohnort
- Email-Adresse

Der Registrierungslink wird vor Veröffentlichung auf der Schulhomepage mit der betreffenden Schule immer abgesprochen. Optionales Feld ist zum Beispiel das Feld „Telefonnummer" sowie „eventuelle Mitteilungen" und Angabe, ob die anmeldende Person oder das Kind Leistungen aus dem Bildungspaket oder andere Förderleistungen z.B. für das Mittagessen erhält. Die Schule kann bestimmen, dass dies freiwillige Angaben sind.
Die allergenen Merkmale liegen der Schulverwaltung vor. Diese veranlasst die Löschung möglicher Phantasieangaben.

Hinsichtlich der allergenen Besonderheiten gilt, dass die Daten nicht ausgewertet werden und auch kein Vorhaben besteht , diese zukünftig auszuwerten. Im Rahmen der Angabe der Telefonnummer kann je Kontakt eine Mobil- und eine Festnetznummer angegeben werden.
Bei der Bankverbindung können die Teilnehmer frei entscheiden, ob Sie Vorauszahlung oder Bankeinzug leisten möchten. Der Antragsteller weist auch auf den Elternabenden auf diese Möglichkeit hin. Ein Wechsel der Zahlweise ist jederzeit durch den Teilnehmer über das I.S.S. Webportal möglich.

6.3.2 Sekundärdaten

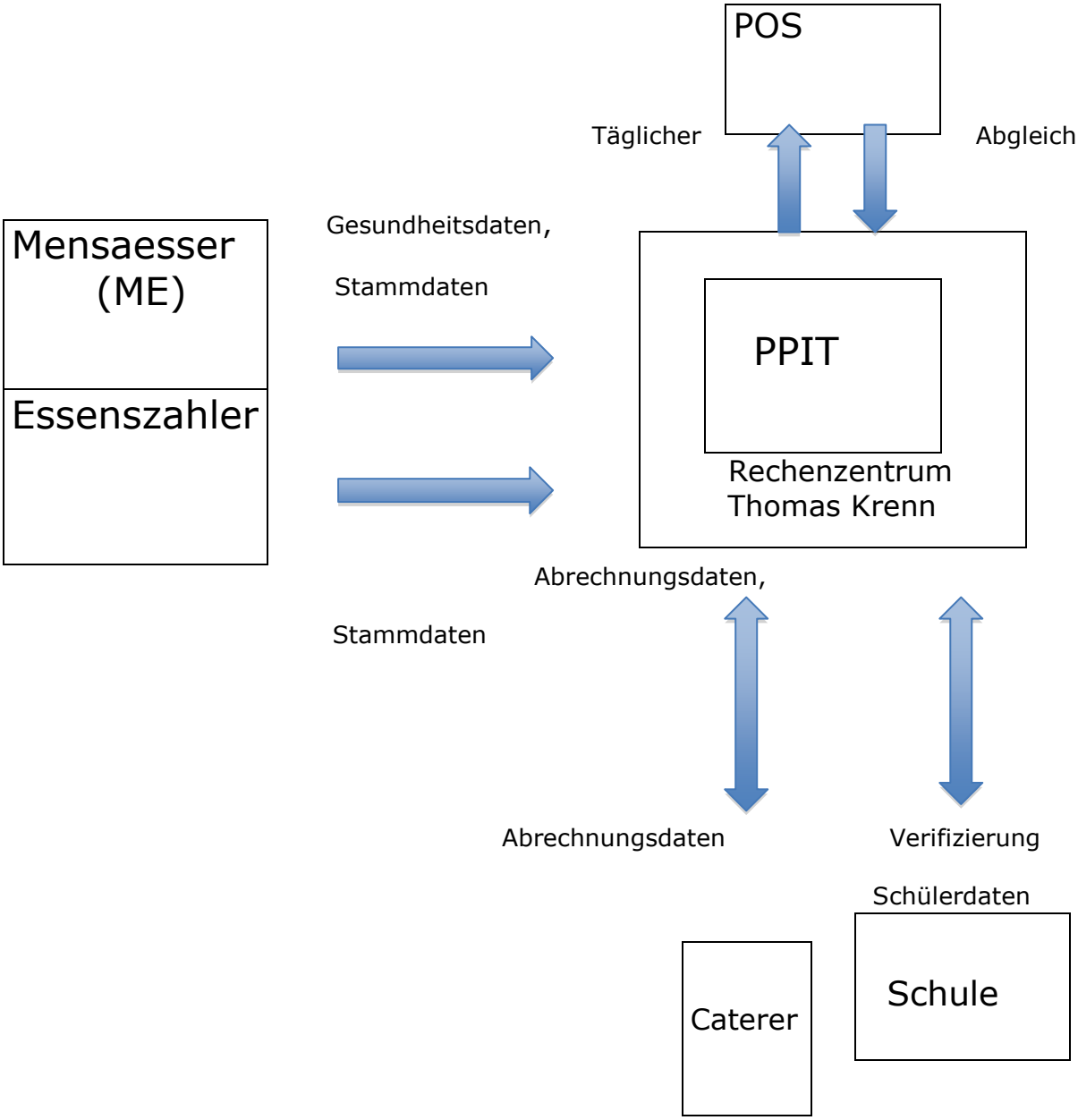
Die An- und Abmeldedaten beinhalten den Benutzer, das Datum und die Uhrzeit der Änderung.
Die Speicherung erfolgt grundsätzlich für 30 Tage. Danach wird der jeweilige Eintrag unwiderruflich gelöscht. Ausgenommen davon sind Änderungen, die durch einen PPIT-Mitarbeiter vorgenommen wurden. Diese Protokollsätze bleiben bis zur Löschung des Teilnehmers erhalten.
Der Eintrag (Benutzer und Datum) ist für PPIT ein Nachweis, dass am Account und folglich mit dem richtigen Passwort eine Anmeldung erfolgte.
Für den Fall, dass ein Anwender sagt, er habe die Essensbestellung, die kurz darauf erfolgte nicht ausgeführt, hat PPIT durch die Login-Protokollierung eine Argumentationsgrundlage.

Die IP-Adresse wird im Rahmen des Webserverprotokolls gespeichert. Diese kann anhand der Login-Routine mit dem Benutzer in Zusammenhang gebracht werden. Die IP-Adressen auf dem Webserver werden im Rahmen des Log-Rotates je nach Serverlast nach 2 bis 7 Tagen gelöscht. Die Protokollierung der IP-Adressen durch den Webserver ist aus Sicherheitsgründen notwendig. Nur mit diesen Daten wären im Falle eines Angriffs eine Rückverfolgung und die Verschärfung der Firewall-Regeln möglich.

Sowohl bei Mitarbeitern (Zugriff über Debitorenverwaltung) als auch bei Teilnehmern (Zugriff über Webportal) werden die Login-Zugänge protokolliert.
Diese Protokolldaten werden nach 30 Tagen gelöscht. Nur die Anzahl der Logins pro Tag bleibt erhalten. Ein darüberhinausgehendes Benutzer-Tracking findet nicht statt. Lediglich Datenänderungen werden wie oben beschrieben protokolliert.

6.4 Datenfluss

Der Datenfluss der I.S.S. Schulmensaverwaltung lässt sich wie folgt darstellen:



7 Eingesetzte Tools

DBMS: Oracle 11 G auf Linux-OS
2 DB: 1 Produktiv, 1 Test

Webserver: Apache

Mailserver: MS Exchange SaaS (E-Mail Support des Service-Centers ist aus dem Zertifizierungsgegenstand herausgenommen).

Tools DB:
PLSQL (Oracle Scriptsprache)
Toad for Oracle

Tools Web:
Php Textedit

8 Anforderungskatalog

Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde: 1.2

9 Zusammenfassung der Prüfergebnisse

9.1 Umsetzung von rechtlichen Anforderungen

Die rechtlichen Anforderungen in Bezug auf die Zulässigkeit der Datenverarbeitung werden eingehalten. Dies bezieht sich insbesondere auf die Einhaltung der §§ 11, 12 LDSG SH.
Die Anforderungen an eine wirksame elektronische Einwilligung im Rahmen der Speicherung der personenbezogenen Daten der Eltern sowie der Schüler werden eingehalten.
Hinsichtlich der Umsetzung der Löschfristen gilt Folgendes:
Hinsichtlich der Primärdaten gilt, dass die handelsrechtlichen Aufbewahrungsfristen beachtet werden. Die Daten, die im Rahmen dieser Pflichten aufzubewahren sind, werden gesperrt.
Nicht aufzubewahrende Daten werden nach Zweckbeendigung gelöscht.
Die Bestelldaten der Mensaesser werden zwei Monate im System vorgehalten, so dass die Betroffenen die Abrechnung prüfen können. Danach werden diese Daten gelöscht.
Die Gesundheitsdaten der Mensaesser werden bei einer Abmeldung vom Verfahren gelöscht.
Die Sekundär (Protokoll-)Daten, die nicht der Nachweispflicht unterliegen, werden nach 30 Tagen gelöscht. Die IP-Adressen auf dem Webserver werden im Rahmen des Log-Rotates je nach Serverlast nach 2 bis 7 Tagen gelöscht.

Nachweispflichtige Protokolldaten werden im Rahmen der gesetzlichen Fristen aufbewahrt. Buchungen, welche älter als 15 Monate sind, werden zum

Schuljahreswechsel für 10 Jahre archiviert. Der direkte Zugriff ist dann nicht mehr möglich.

Die Daten sollen nach 10 Jahren gelöscht werden, dies ist allerdings bis jetzt noch nicht umgesetzt, da es das Unternehmen noch nicht zehn Jahre lang gibt. Die Löschfrist wird aber im Laufe der Zertifizierungsfrist innerhalb von zwei Jahren so umgesetzt werden.

9.2 Datensparsamkeit

In allen Modulen wurde darauf geachtet, nur die für die Zweckerfüllung erforderlichen Daten zu erheben. Im I.S.S. Webportal besteht die Möglichkeit der weiteren Dateneingabe, zum Beispiel der Angabe der Telefonnummer, um diesen Kontaktweg ebenfalls zu nutzen. Die Datenerhebungen sind in diesem Fall freiwillig mit der entsprechenden Kennzeichnung.
Nicht mehr benötigte Daten werden automatisch unwiderruflich gelöscht.
Es besteht ein detailliertes Konzept zur Löschung der Daten in den Nutzungsbedingungen sowie ein detailliertes Berechtigungskonzept.

9.3 Datensicherheit

Der Hersteller hat durch technische Maßnahmen dafür Sorge getragen, dass nur vier ausgewählte Mitarbeiter direkten Zugriff auf das System haben. Nur mit entsprechender Zugriffsberechtigung kann auf die Daten zugegriffen werden.
Die Schule hat keinen direkten Zugriff auf die Datenbank. Der Zugriff der Debitoren, z.B. auf Speisepläne, erfolgt nur über die Debitorenverwaltung.

Es erfolgt eine Protokollierung von jeglichen Änderungen, die durch eine Applikation erfolgt sind.
Die Server werden in einem Rechenzentrum mit ausreichenden Zugangs- und Zugriffskontrollen betrieben.
In der I.S.S. Schulmensaverwaltung wird SSL 2048bit per stunnel eingesetzt.
Jede Nacht wird ein Dump und eine Rman-Sicherung erzeugt. Diese werden auf ein Storage übertragen, das mit dem Server über dessen zweite Netzwerkkarte verbunden ist. Ein Zugriff auf diesen Storage ist nur über den Server möglich und zusätzlich per ssh geschützt. Jede Sicherung wird nach 7 Tagen auf dem Storage gelöscht.

9.4 Beachtung der Betroffenenrechte

Die Anforderungen hinsichtlich der Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung werden eingehalten. Über das I.S.S. Webportal haben die Eltern als Essenszahler die Möglichkeit, die eingegebenen (Stamm-)Daten zu überprüfen, zu ändern und zu löschen.
Eine aktuelle Produktbeschreibung liegt vor (Stand Oktober 2012). In dieser werden das I.S.S. Webportal, die I.S.S. Debitorenverwaltung und das I.S.S. POS beschrieben.
In jedem Abschnitt wird beschrieben, welche Daten erhoben und an welchem Ort sie gespeichert werden. Anwender und Betroffene werden über die Zugriffsmöglichkeiten sowie über die einzelnen Datenflüsse informiert. In technischer Hinsicht erfolgt eine Aufklärung über die Schnittstellen und die Ausfallsicherheit der Server. Die Eltern/Essenszahler werden durch einen Elternabend und durch die Dokumentation im Websystem über das Verfahren informiert. Eltern, die nicht an einem angekündigten Elternabend teilnehmen können, werden durch einen Formbrief informiert, der im Detail zum Nutzen und Einsatz des Systems Auskunft gibt sowie durch genaue Anwenderhilfen den Einsatz unterstützt. Des Weiteren wird die Service-Rufnummer angegeben, unter der fragende Eltern einen persönlichen Ansprechpartner erreichen, mit dem alle Fragen geklärt werden können.

Da die Eltern als Essenszahler die Daten selbst in die Maske des Webportals eingeben, bestimmen sie somit auch darüber, welche Daten erhoben werden.
Die Eltern werden in der Datenschutzerklärung darüber informiert, dass ein Recht auf Auskunft sowie ein Recht auf Berichtigung, Sperrung und Löschung der gespeicherten Daten besteht.
Aufgrund der Tatsache, dass die persönlichen Stammdaten individuell für den einzelnen Teilnehmer einsehbar sind, kann der Erziehungsberechtigte/Schüler über den durch Passwort geschützten Zugangsbereich die eigene Historie der bestellten und abgerechneten Essen nachverfolgen. Wünscht der Erziehungsberechtigte/Schüler eine Änderung bzw. hat eine Nachfrage, so wendet er sich an die PPIT/Servicecenter. Bei diesen Auskünften kommen ebenfalls die Einträge aus den Stammdaten zur Anwendung – dort sind die jeweils individuell bestimmten Personen eingetragen, die Zugang zu den Daten haben. Spezielle Anfragen, die nicht im Rahmen des Stammdatenblattes einsehbar sind, werden über gesondert geprüft über den Datenschutzbeauftragten der PPIT bearbeitet.

Die personenbezogenen Daten von Mensaessern sowie Essenszahlern sind durch bestehende Verträge zur Auftragsdatenverarbeitung zwischen PPIT und dem Rechenzentrum, PPIT und Schule sowie Schule und Caterer abgesichert. Zwischen PPIT und dem Caterer besteht kein Auftragsdatenverarbeitungsvertrag, sondern es werden Daten im Rahmen des Weisungsrechts der Schule übermittelt.

10 Förderung des Datenschutzes

Das Produkt stellt dem Nutzer unterschiedliche Möglichkeiten zur Nutzung des Moduls zur Verfügung. Eine Teilnahme ist grundsätzlich freiwillig.
Das Hochladen eines Fotos ist ebenfalls freiwillig. Das Foto wird nicht abgefragt, aber auf Wunsch der Schule kann dieses implementiert werden. Die Schule ist verpflichtet, zu prüfen, ob dies rechtmäßig ist.
Dem Nutzer wird eine angemessene Produktbeschreibung zur Verfügung gestellt, welche für den Nutzer verständlich beschrieben ist. Zudem führt ein Handbuch durch die notwendigen Schritte der Registrierung und Dateneingabe.

11 Votum

Hiermit bestätige ich, dass das IT-Produkt I.S.S. Schulmensaverwaltung und der dazugehörende IT-Service mit Stand Juni 2013 (Version 6.0) den Rechtsvorschriften über den Datenschutz und die Datensicherheit entsprechen. Die ausführliche Analyse liegt bei.

Ort, Datum	Unterschrift Leiter der Prüfstelle