Entwicklung eines elektronisch unterstützten Schulungssystems für die Sensibilisierung zum Thema Datenschutz

Praxisprojektarbeit zur Erlangung des Moduls Praxisprojekt
Bachelor of Science im Studiengang Wirtschaftsinformatik
an der Fakultät für Informatik und Ingenieurwissenschaften
der Technischen Hochschule Köln

vorgelegt von:	Marco Nentwig
Matrikel-Nr.:	1111 7198
Adresse:	Hauptstraße 121
	51570 Windeck
	Marco.Nentwig@smail.th-koeln.de

eingereicht bei: Prof. Dr. Birgit Bertelsmeier

Gummersbach, 01.02.2021

Erklärung

Ich versichere, die von mir vorgelegte Arbeit selbstständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer oder der Verfasserin/des Verfassers selbst entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

Ort, Datum

Rechtsverbindliche Unterschrift

Kurzfassung/Abstract

Titel: Entwicklung eines elektronisch unterstützten Schulungssystems für die Sensibilisierung zum Thema Datenschutz

Zusammenfassung: Ziel dieser Arbeit ist die Entwicklung eines E-Learning Systems, welches als asynchrones und flexibles Online-Format frei zugänglich ist. Nach einer Zusammenfassung der wichtigsten theoretischen und rechtlichen Schulungsthemen, wird das System konzipiert und prototypisch entwickelt. Die Zielgruppe des Systems sind in erster Linie Einzelpersonen und Arbeitnehmer, welche eine Datenschutzschulung aufgrund von Nachweispflichten des Datenschutzgrundgesetzes benötigen.

Schlüsselwörter: E-Learning, Datenschutz, Online-Schulung, DSGVO

Title: Development of an electronically supported training system to raise awareness on the subject of data protection

Abstract: The goal of this thesis is the development of an e-learning system, which is publicly available as an asynchronous and flexible online format. After a summary of the most important theoretical and legal training topics, the system is designed and prototyped. The target group of the system are primarily individuals and employees who need data protection training due to the obligation to provide evidence under the General Data Protection Regulation.

Keywords: E-Learning, Data protection, Online training, GDPR

Inhalt

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

Das folgende Kapitel gibt einen Überblick über die Vorstellung und das Ziel des Praxisprojektes. Die Motivation beschreibt die derzeitige Ausgangssituation und die treibende Idee hinter der Durchführung. Die Zielsetzung behandelt die Anforderungen an das Endprodukt, welches durch dieses Projekt umgesetzt werden soll.

1.1 Motivation

Am 25. Mai 2016 ist die EU-Datenschutz-Grundverordnung in Kraft getreten. Zwei Jahre konnten sich Unternehmen auf die neue Verordnung vorbereiten, welche seit dem 25. Mai 2018 gültig ist.[1]

Viele Unternehmer waren anfangs verunsichert, welches Ausmaß die neue Verordnung mit sich bringt. Die meisten Großunternehmen haben sich weitreichend mit dem Thema befasst, eigene Abteilungen für den Datenschutz gebildet und unterrichten ihre Mitarbeiter in regelmäßigen Abständen. Kleine und mittelständige Unternehmen besitzen in den meisten Fällen nicht die finanziellen Mittel und keine ausreichenden Kapazitäten, um einen Datenschutzbeauftragten zu bestellen. In Folge dessen wird der Datenschutz vernachlässigt und rückt in Vergessenheit. Sollte es jedoch zu einem schweren datenschutzrechtlichen Vorfall kommen, könnte dieser ein Unternehmen zur Existenzbedrohung führen.

Damit Arbeitnehmer wissen, wie sie sich zu verhalten haben und was genau es mit dem Datenschutz auf sich hat, müssen diese in regelmäßigen Abständen durch einen Experten in dem Fachgebiet geschult werden.

Im Zusammenhang mit Datenschutz wird das E-Learning immer mehr zum Trend. E-Learning kann einfacher in den Arbeitsalltag jedes Einzelnen integriert oder auch von Zuhause aus erledigt werden. Präsenzveranstaltungen hingegen müssen aufwendig geplant werden, da alle Mitarbeiter zu einem bestimmten Zeitpunkt anwesend sein müssen. Dies ist selbst in kleinen und mittelständigen Unternehmen nicht immer umsetzbar.

Als „Geprüfter Datenschutzbeauftragter und Zertifizierte Fachkraft nach BDSG und DSGVO“ besitze ich die notwendigen Fachkenntnisse nach BDSG[2] und DSGVO[3] um Unternehmen als Datenschutzbeauftragter zur Seite zu stehen und passende Schulungen durchzuführen. Hierbei könnte ein elektronisch unterstütztes Lernsystem den Lernerfolg, die Kosten, sowie die Protokollierung der Durchführung für Unternehmen verbessern.

Da bereits viele Datenschutzunternehmen kostspielige Mitarbeiter-Schulungen zum Thema Datenschutz anbieten, soll das System kostenlos und zur freien Verfügung im Internet angeboten werden.

[1] [DSGVO] Vgl. § 99

[2] [BDSG] Vgl. § 40 Abs. 6

[3] [DSGVO] Vgl. § 37 Abs. 5

1.2 Zielsetzung

Die vorliegende Arbeit befasst sich mit der Möglichkeit, durch elektronisch unterstütztes Lernen, die Sensibilisierung zum Thema Datenschutz zu optimieren.

Ziel ist es ein System zu entwickelt, welches als asynchrones und flexibles Online-Format frei zugänglich ist. Hierbei werden alle wichtigen Themen rund um den Datenschutz, welche in erster Linie für Arbeitnehmer relevant sind, als Schulungsunterlagen bereitgestellt. Grundsätzlich sollen drei wesentliche Ziele durch die Schulung abdeckt werden, Arbeitnehmer zu datenschutzkonformen Verhalten zu befähigen, die Bereitschaft zu datenschutzkonformen Verhalten zu fördern und ein Bewusstsein für datenschutzrechtliche Probleme zu schaffen. Weiterhin sollen die Schulungsthemen fachfremden Personen verständlich gemacht werden, ohne im Detail auf einzelne Gesetze und Normen einzugehen.

Nach Bearbeitung des Lernmaterials steht ein Test zur Verfügung. Bei erfolgreichem Abschluss des Lernerfolgs wird ein Zertifikat für die jeweilige Person als persönlichen Nachweis, sowie für die Unternehmen zur Protokollierung der Rechenschaftspflicht[4] erstellt.

Idealerweise können regelmäßige Präsenzveranstaltungen zu Schulungszwecken für den Datenschutz, welche mit zeitintensiver Planung im Zusammenhang stehen, komplett ersetzt werden.

1.3 Gliederung der Arbeit

Diese Arbeit behandelt im Kapitel zwei zunächst die theoretischen Teile der Schulungsthemen für die zu erarbeitende praktische Umsetzung der Schulung. Daher wird zu Beginn des Kapitels 2.1 auf die erforderlichen Datenschutzbestimmungen eingegangen. Das Kapitel 2.2 ergänzt die Schulungsthemen um Sicherheitsaspekte und Verhaltensregeln im Unternehmen.

Im Kapitel drei wird die Konzeption des E-Learning Systems vorgestellt. Zunächst werden in Kapitel 3.1 alle Techniken beschrieben, welche als Grundlagen des Aufbaus des Systems gelten. Anschließend werden in Kapitel 3.2 die verwendeten Hilfsmittel erläutert, welche zur Umsetzung genutzt wurden.

Das vierte Kapitel behandelt die prototypische Entwicklung des E-Learning Systems. Hier wird zu nächst in Kapitel 4.1 das Back-End mit den geplanten Funktionen und der dahinterliegenden Datenbank beschrieben. Das zweite Kapitel zu 4.2 beschreibt das Design, die Entscheidungen und den Aufbau des Front-End und die rechtlichen Aspekte für die Nutzung des Systems. Im Kapitel 4.3 wird erläutert, wie auf das System zugegriffen werden kann. Eine Dokumentation der Aufwendungen spiegelt sich in Kapitel 4.4 wieder.

[4] [DSGVO] Vgl. § 5 Abs. 2

Das fünfte und letzte Kapitel evaluiert welche Anforderungen umgesetzt werden konnten und ob ein Verbesserungspotential entsteht. Abschließend wird ein Fazit gezogen und die Zukunft des Systems betrachtet.

2 Theorie der Schulungsthemen

Das folgende Kapitel gibt einen Überblick über die Theorie und Inhalte der unterschiedlichen Schulungsthemen. Die Themen sind speziell für Arbeitnehmer ausgewählt und sollen als Grundlagen, Sensibilisierung und Verhaltensregeln dienen. Fachgerechte Schulungen durchzuführen unterliegt den Aufgaben eines zertifizierten Datenschutzbeauftragten.

In den Unterkapiteln zu 2.1 Schulung der Datenschutzgrundlagen wird allgemein auf die erforderlichen Datenschutzbestimmungen eingegangen. Sie erläutern unter anderem was unter Datenschutz zu verstehen ist, welche Gesetze es einzuhalten gilt, wer für den Datenschutz zuständig ist, wie Daten zu verarbeiten sind, welche Rechte natürliche und welche Pflichten juristische Personen haben, sowie welche Konsequenzen es bei Nichteinhaltung gibt.

Das zweite Unterkapitel zu 2.2 schneidet die IT-Sicherheit, sowie speziellere Datenschutzschulungen an. Hier werden unter anderem die Grundsätze der IT Sicherheit erläutert, Verhaltensregeln für die Nutzung von Computersystemen aufgestellt, den Umgang mit Passwörtern vorgeschrieben und Empfehlungen für einen besseren Schutz im Unternehmen vermittelt.

2.1 Schulung der Datenschutzgrundlagen

2.1.1 Datenschutz im Allgemeinen

Im Laufe des Lebens erzeugt jede Person viele Informationen. Diese werden in Form von Daten in unterschiedlichen Bereichen von Verwaltung und Wirtschaft erhoben, verarbeitet und gespeichert. Die Verarbeitung dieser Daten birgt Gefahren für die Persönlichkeitsentwicklung und die Persönlichkeitsentfaltung. Ein Individuum kann sich nicht mehr selbst ein Bild für die Umwelt erschaffen, wenn es nicht weiß, was andere Menschen bereits über seine Person wissen. [5]

Datenschutz im Allgemeinen ist der Schutz der eigenen personenbezogenen Daten. Es soll sichergestellt werden, dass jede natürliche Person der rechtmäßige Eigentümer ihrer eigenen Daten bleibt und selbst entscheiden kann, was mit ihnen geschieht.

Um den Schutz dieser Daten gegen Missbrauch zu gewährleisten, wurden im Laufe der Zeit verschiedene Gesetze auf europäischer und nationaler Ebene verabschiedet. Das bekannteste ist das *Grundgesetz*. „Das Grundgesetz gewährleistet jeder Bürgerin und jedem Bürger das Recht, über Verwendung und Preisgabe seiner persönlichen Daten zu bestimmen (Grundrecht auf informationelle Selbstbestimmung). Geschützt werden also nicht Daten, sondern die Freiheit der Menschen, selbst zu entscheiden, wer was

[5] [LDI] Vgl. Was ist Datenschutz [online]

wann und bei welcher Gelegenheit über sie weiß.“[6] Die wichtigsten Gesetze im europäischen Datenschutzrecht sind die *EU-Datenschutz-Grundverordnung* (DSGVO), die *e-Privacy-Verordnung* (ePrivacy-VO) und die *Universaldienstrichtlinie* (RL 2002/22/EG). Im nationalen Recht sind in vielen Gesetzen, Teile für den Datenschutz enthalten, diese sind unter anderem das *Bundesdatenschutzgesetz* (BDSG), das *Betriebsverfassungsgesetz* (BetrVG), das *Informationsfreiheitsgesetz* (IFG), das *Strafgesetzbuch* (StGB), das *Telekommunikationsgesetz* (TKG), *Telekommunikations-Überwachungsverordnung*(TKÜV) oder das *Telemediengesetz* (TMG).[7]

2.1.2 Akteure und Verantwortliche

Im Bereich des Datenschutzes gibt es verschiedene Akteure mit unterschiedliche Pflichten und Rechte. Die zwei Hauptakteure sind einerseits der *Verantwortliche* und anderseits der *Betroffene*. Der Verantwortliche verarbeitet Daten, welche der Betroffene bereitstellt. Als Verantwortlicher gelten unter anderem natürliche und juristische Personen, Unternehmen, Behörden oder staatliche Einrichtungen. Als Betroffener werden in den meisten Fällen natürliche Personen, Kunden, Mitarbeiter und Lieferanten bezeichnet. Die Verantwortlichen haben die Pflicht den Datenschutz bei der Verarbeitung der Daten zu gewährleisten. Die Betroffenen haben das Recht über die zu verarbeiteten Daten zu bestimmen.

Ein Verantwortlicher kann einen *Datenschutzbeauftragten* bestellen, welcher als erster Ansprechpartner in datenschutzrechtlichen Angelegenheiten im Unternehmen gilt. Sollten umfangreiche Verarbeitungen personenbezogener Daten beim Verantwortlichen stattfinden, mindestens 20 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sein oder werden sensible Daten verarbeitet, besteht die Pflicht einen Datenschutzbeauftragten zu benennen. Dieser überwacht den Datenschutz im Unternehmen und ist beispielsweise für die Schulungen der Mitarbeiter zuständig. Trotz bestellten Datenschutzbeauftragten liegt die allgemeine Verantwortung weiterhin beim Verantwortlichen.

Externe Dienstleistungsunternehmen, welche im Auftrag des Verantwortlichen Daten verarbeiten, werden *Auftragsverarbeiter* oder auch *Dritte* genannt. Diese Dienstleistungen können von einer externen Lohnverrechnung bis hin zur Bereitstellung eines Internetauftritts gehen. Im Allgemeinen gilt, werden in irgendeiner Weise personenbezogene Daten von externen Unternehmen gesichtet oder anderweitig verarbeitet, liegt eine Auftragsverarbeitung vor. Verantwortlicher und Auftragsverarbeiter müssen einen Auftragsverarbeitungsvertrag abschließen, damit das externe Unternehmen die Einhaltung und Haftung des Datenschutzes garantiert.

[6] [BFDI] Was ist Datenschutz [online]

[7] [DSR] Vgl. DatSchR Datenschutzrecht S.1-2

Zur Überwachung und Durchsetzung des Datenschutzes wurden Aufsichtsbehörden und Landesdatenschutzbeauftragte berufen. Diese Behörden gelten als Ansprechpartner für Beschwerden, Fragen und Aufklärungen im jeweiligen Hoheitsgebiet.[8]

2.1.3 Personenbezogene Daten

Der Datenschutz soll personenbezogene Daten schützen. Diese Daten besitzen die Eigenschaft Rückschlüsse auf einzelne Personen und ihr Verhalten zu ziehen.[9] Hiermit gemeint sind zum einen direkte Informationen, wie Name, postalische Anschrift und Telefonnummer. Zum anderen aber auch personenidentifizierbare Informationen, welche einen Bezug zu der Person herstellen, wie körperliche Merkmale, Sachverhalte, KFZ-Kennzeichen. Es ist bedeutungslos in welcher Form die Daten vorhanden sind, auch Papiere, wie schriftliche Fragebögen, Akten oder Notizen können personenbezogene Daten darstellen.

Eine besondere Kategorie der personenbezogenen Daten stellen die sensiblen Daten dar. Sensible Daten geben unter anderem Aufschluss über rassische und ethnische Herkunft, politische und religiöse Meinungen, biometrische und gesundheitliche Daten, Sexualleben oder auch Gewerkschaftszugehörigkeit. Diese Daten dürfen nur in besonderen Umständen oder mit explizierter Einwilligung verarbeitet werden. [10]

2.1.4 Grundsätze der Verarbeitung

Bereits bei der Erhebung von personenbezogen Daten muss auf die Einhaltung von gewissen Grundsätzen der Verarbeitung geachtet werden. Prinzipiell ist das Verarbeiten von personenbezogenen Daten verboten. Erst durch die *Rechtmäßigkeit*, durch Berufung einer gültigen Rechtsgrundlage, dürfen Daten nach Treu und Glaube verarbeitet werden.

Natürliche Personen sollen ganz genau wissen, welche Daten von wem und wofür erhoben werden, sowie welche Rechte sie in den jeweiligen Fällen besitzen. Eine gewisse *Transparenz* und umfassende *Informationspflicht* des Verantwortlichen müssen erfolgen.

Jeder Verarbeitungsvorgang muss einer eindeutigen *Zweckbindung* zugewiesen sein. Daten zur Vertragserfüllung dürfen beispielsweise nicht einfach an eine Marketingaktion gekoppelt werden. Ohne explizite Einstimmung dürfen bereits erhobene Daten nicht für unterschiedliche Zwecke entfremdet werden.

Auch der Umfang der Daten muss für einen Zweck bestimmbar sein. Im Sinne einer *Datenminimierung* dürfen nur zwingend notwendige Daten, zur Erfüllung des Zwecks erhoben werden. Unnötige Altbestände müssen gelöscht oder vernichtet werden.

[8] [OHF] Vgl. Verarbeiter [online]

[9] [STB] Vgl. DSGVO-Bibel, Kap. 1, S. 28

[10] [DSGVO] Vgl. § 9 Abs. 1

Verwendete Daten müssen immer auf dem aktuellsten Stande sein, denn falsche Informationen können nachteilig wirken und Fehler verursachen. Die *Richtigkeit* ist zu gewährleisten und Fehlinformationen zu korrigieren.

Im Vorfeld sollte für jeden Zweck bestimmt werden, für wie lange die notwendigen Daten gespeichert werden. Die *Speicherbegrenzung* schreibt vor, es ist festzulegen, zu welchem Zeitpunkt die Daten gelöscht werden. Das Löschen ist so durchzuführen, dass eine Wiederherstellung der Daten nicht mehr möglich ist. In den meisten Fällen gibt es gesetzliche Aufbewahrungspflichten, an denen die *Speicherbegrenzung* angelehnt werden kann.

Um die Sicherheit bei der Verarbeitung zu garantieren, muss die *Integrität und Vertraulichkeit* gewährleistet werden. Es sind technische und organisatorische Maßnahmen bereitzustellen, welche den Zugang für unbefugte Dritte versperrt und die Daten vor äußeren Einflüssen schützt. [11]

2.1.5 Rechtmäßigkeit der Verarbeitung

Neben den Grundsätzen ist auch die Rechtmäßigkeit der Verarbeitung zu prüfen. Nur wenn ein Erlaubnistatbestand vorliegt, darf die Verarbeitung überhaupt stattfinden. Die Verarbeitung ist immer dann rechtmäßig, wenn eine *Einwilligung der Person* vorliegt. Diese muss freiwillig, bestimmt, in informierter Weise, ausdrücklich und unmissverständlich abgegeben bzw. unterschrieben und nachweisbar aufgehoben werden.[12]

Um den Handel zu erleichtern, ist die Verarbeitung zur *Erfüllung eines Vertrages* und auch ihre *vorvertraglichen Maßnahmen* erlaubt. Es würde sich schwer erweisen, beispielsweise im Handwerk, Buchhaltung, Dienstleistungen oder Lieferung, ohne personenbezogene Daten auszukommen.

Zur *Erfüllung von rechtlichen Verpflichtung* ist die Datenverarbeitung grundsätzlich erlaubt. Handels- und Steuergesetze erfordern umfassende Dokumentations- und Aufbewahrungsfristen und stehen somit in enger Konkurrenz zu Löschfristen.

In Fällen von Katastrophen, die Gesundheit oder Leben eines Menschen beeinträchtigen können, ist die Weitergabe von Daten rechtmäßig. Dies dient dem Schutz und zur *Wahrung lebenswichtiger Interessen* von Personen.

Zur *Wahrnehmung der Aufgaben aus öffentlichem Interesse* oder auch der *Ausübung öffentlicher Gewalt* ist es zwingend notwendig personenbezogene Daten zu speichern. Öffentliche Dienste, wie Polizei, Städte oder auch Gemeinden dürfen Ihre Daten ohne Einwilligung verarbeiten, solange es dem Zweck dient.

Weiterhin dürfen personenbezogene Daten unter Abwägung *des berechtigten Interesses* verarbeitet werden. „Das berechtigte Interesse umfasst das rechtliche, tatsächliche,

[11] [ADP] Vgl. Datenschutz in der Praxis, S. 59-70

[12] [LDI] Vgl. Einwilligung in die Verarbeitung personenbezogener Daten [online]

wirtschaftliche oder ideelle Interesse des Verantwortlichen, wobei eine umfassende Interessenabwägung insbesondere anhand des Zwecks der Datenverarbeitung sowie der Art und des Inhalts der betroffenen Daten erfolgen muss. Dabei dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.“[13]

2.1.6 Rechte der Betroffenen

Jede betroffene Person kann von gewissen Rechten Gebrauch machen, falls ein Unternehmen Daten über sie verarbeitet. Um überhaupt feststellen, welche Daten über einen gespeichert sind, kann das *Recht auf Auskunft* ausgeübt werden. Der Verantwortliche muss der betroffenen Person alle Verarbeitungszwecke, die Kategorien und personenbezogener Daten, sowie alle Empfänger, die Dauer und die Herkunft ihrer Daten preisgeben. Hierfür wird dem Verantwortlichen eine Frist von maximal einem Monat bereitgestellt.

Sollten falsche bzw. unrichtige Informationen in Umlauf geraten sein, kann das *Recht auf Berichtigung* durchgesetzt werden. Hierbei kann ein Betroffener veranlassen, dass seine Daten vervollständigt bzw. berichtigt werden. Der Verantwortliche hat somit Sorge zu tragen, alle internen und externen Empfänger zu Benachrichtigen und die Daten ändern zu lassen.

Um unnötiges Massenspeichern zu verhindern, wurde das *Recht auf Löschung* bzw. das *Recht auf Vergessenwerden* eingeräumt. Bei Beendigung des Zwecks, müssen alle nicht mehr benötigten Daten vernichtet werden. Auch wenn die betroffene Person die Verarbeitung nicht mehr wünscht oder einen Widerspruch einlegt, muss der Verantwortliche alle verarbeiteten Daten rechtmäßig vernichten. Es muss berücksichtigt werden, dass nicht alle Daten bedenkenlos gelöscht werden können, da die gesetzlichen Aufbewahrungsfristen Vorrang haben.

Bei Unklarheiten bezüglich der Verarbeitung kann das *Recht auf Einschränkung der Verarbeitung* bzw. *Recht auf Sperrung* genutzt werden. Gibt es Schwierigkeiten bei der Richtigkeit, Rechtmäßigkeit, Zweckbindung oder eines unrechtmäßigen Widerspruchs, müssen die entsprechenden Daten für den Zeitraum gesperrt werden. Der Betroffene und alle beteiligte Stellen sind über die Sperrung, sowie über die Aufhebung zu informieren.

Zu den weiteren Rechten gehört die *Mitteilungspflicht.* Wie bereits erwähnt, muss der Verantwortliche bei Berichtigung, Löschung oder Sperrung der personenbezogenen Daten den Betroffenen und allen internen sowie externen Empfänger benachrichtigen.

Um einen leichten Wechsel von beispielsweise Verträgen zu ermöglichen, kann das *Recht auf Datenübertragbarkeit* genutzt werden. Demnach muss der Verantwortliche alle Daten in einem strukturierten, gängigen und maschinenlesbaren Format entweder bereitstellen oder bei Beauftragung einem anderen Verantwortlichen direkt übermitteln.

[13] [ICS] Rechtmäßigkeit der Verarbeitung [online]

Weiterhin haben Betroffene das Recht nicht *ausschließlich automatisierten Entscheidungen bzw. Profiling* unterworfen zu sein. Beispielweise bei einem online beantragten Kredit, dürfen die Entscheidungen, ob ein Kredit gewährleistet wird oder nicht, nicht alleine aufgrund von Algorithmen entschieden werden.

Falls ein Betroffener nicht zufrieden mit der Verarbeitung seiner Daten ist, kann sich auf das *Widerspruchsrecht* gestützt werden. Dies ist meistens bei Zwecken der Direktwerbung oder eines Profilings sehr nützlich. Der Verantwortliche darf die Daten für den gewünschten Zweck nicht mehr nutzen.[14]

Bei Fragen über die Verarbeitung hat ein Betroffener immer das *Recht den Datenschutzbeauftragten zu konsultieren* und bei berechtigten Beschwerden auch das *Recht auf Beschwerde bei einer Aufsichtsbehörde*.[15]

2.1.7 Konsequenzen, Bußgelder und Strafen

Bei Verstößen gegen das geltende Datenschutzrecht können verschiedenen Strafen verhängt werden. Je nach Schweregrad eines Vorfalls kann gegen unterschiedliche Gesetze verstoßen werden. Die derzeitige Höchststrafe bei einer Geldstrafe beträgt bis zu 20 000 000 Euro oder 4% des gesamten, weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens, wobei der höhere Betrag genommen wird. [16]

Es können aber auch Freiheitsstrafen von bis zu drei Jahren verhängt werden, wenn wissentlich, unberechtigt, nicht allgemein zugängliche personenbezogene Daten beispielsweise an Dritte weitergegeben werden.[17]

Im Vergleich zu den gesetzlichen Strafen, die meist nur gegen den Verantwortlichen wirken, können auch unternehmensspezifische Strafen bei Arbeitnehmern erfolgen. Bei leichten Verstößen oder dem Ignorieren von festgelegten Richtlinien können Abmahnungen verhängt werden. Bei schwerwiegenderen Verstößen können Arbeitnehmer unter besonderen Umständen, im Einzelfall außerordentlich und auch fristlos, gekündigt werden.

Die Bekanntmachung eines Datenschutzverstoßes schädigt das gesamte Unternehmen. Das Unternehmen erleidet einen starken Reputationsverlust, dessen Auswirkung bis zu einem vollständigen Verlust des Vertrauens der Kunden reichen kann. Somit wird oft nicht nur eine Strafe verhängt, sondern das Unternehmen hat noch mehr Verluste durch den Abgang von Kunden.

Daher ist es ratsam sich im Vorfeld abzusichern, zahlreiche Versicherungsunternehmen bieten spezielle „Cyber-Versicherungen“ für Unternehmen an, welche den Datenschutz,

[14] [ADP] Vgl. Datenschutz in der Praxis, S. 73-88

[15] [DSGVO] Vgl. § 77 Abs. 1

[16] [DSGVO] Vgl. § 83 Abs. 5

[17] [BDSG] Vgl. § 42 Abs. 1

sowie Reputationsschäden abdecken. Auch natürliche Personen können gegen Cyberkriminalität abgesichert werden. Häufig gibt es in jüngeren Policen von privaten Haftpflichtversicherung Klauseln für den speziellen Schutz, dies sollte jedoch explizit mit dem Versicherungsberater abgeklärt werden.

2.2 Ergänzende Fachschulungen

2.2.1 Grundsätze der IT-Sicherheit

Der Begriff IT Sicherheit beschreibt einen umfassenden Zustand, welcher das Ziel hat die informationstechnologische Umgebung frei von Gefahren und Risiken zu halten. „Einen absoluten risiko- bzw. gefahrenfreien Zustand gibt es nicht. Daraus erfolgt, dass es auch eine hundertprozentige Sicherheit nicht geben kann. Sicherheit ist demnach immer nur als relativer Zustand der Gefahrenfreiheit anzusehen, d.h. bezogen auf eine bestimmte Situation, einen bestimmten Zeitraum und bestimmte Rahmenbedingungen.“[18]

Im Folgenden werden die drei grundlegenden Sicherheitskriterien kurz erläutert, welche die meisten Aufgaben der IT-Sicherheit zusammenfassen kann.

Um Hard- und Software überhaupt benutzen zu können, muss die *Verfügbarkeit* gewährleistet sein. Diese sagt im Allgemeinen aus, dass IT-Dienste verfügbar sind und genutzt werden können. Als Schutzmaßnahmen werden in den meisten Fällen Backup-Systeme, unterbrechungsfreie Stromversorgungen und Notfallpläne eingesetzt. In der Regel wird die Verfügbarkeit prozentual berechnet. Die nachfolgende Tabelle gibt einen Überblick, in welchem Maß bereits eine 99%tige Verfügbarkeit schädlich sein kann.

Verfügbarkeit	Ausfall pro Jahr
90 %	36,5 Tage
95 %	18,5 Tage
99 %	3,65 Tage
99,9 %	8,76 Stunden
99,99 %	52,56 Minuten
99,999 %	5,26 Minuten

Tabelle 1: Verfügbarkeitstabelle

Als zweites Sicherheitskriterium wird die *Integrität* behandelt. Diese sagt aus, dass Informationen nicht unbefugt und unbemerkt verändert werden dürfen. Als Schutzmaßnahe werden beispielsweise Verschlüsselungen, Signaturen, Dokumentenmanagement und sichere Übertragungsmedien genutzt.

Das dritte Sicherheitskriterium bildet die *Vertraulichkeit*. In einem Unternehmen existieren viele vertrauliche Informationen, welche nur von bestimmten Personengruppen verarbeitet werden dürfen. Die Vertraulichkeit beschreibt ein Maß, inwieweit gewährleistet ist, dass die Informationen auch nur an die für sie Bestimmte gelangen und kein Dritter Einblick in diese bekommt. Zutritts- und Zugriffkontrollen, Passwortrichtlinien, Verschlüsselungen, Sperrungen und Protokollierungen werden als Schutzmaßnahmen eingesetzt.

[18] [SKI] Datenschutz in der Praxis, S. 14-18

2.2.2 Systemsicherheit

Um ein System sicher zu halten benötigt es die Aufsicht von Menschen. Ein Administrator richtet im Normalfall ein System so ein, dass es von Laien leicht benutzbar und bei normaler Benutzung sicher ist. Es braucht jedoch regelmäßige Pflege und Aufmerksamkeit, um den Schutz auch weiterhin zu gewähren. Es gelten somit spezifische Verhaltensregel für Computersysteme:

- Computersysteme bei Nichtbenutzung bzw. Beendigung der Arbeit immer ganz herunterfahren, nicht im Standby Modus lassen
- Ausnahme bei nur kurzfristigen Verlassen kann der Computer auch gesperrt werden
- Keine Passwörter auf Papier dokumentieren, besser einen Passwortmanager nutzen
- System- und Virenschutzsoftware mit Sicherheitsupdates immer auf den neusten Stand bringen
- Emails kritisch überprüfen, auch wenn diese von vermeintlich vertrauten Personen gesendet wurden
- Heruntergeladene Inhalte und Anhänge immer erst überprüfen
- Nicht eigenständig Software installieren
- Bei Verdacht auf einen Virenbefall, dem zuständigen Administrator melden und das System in der Zeit nicht weiter benutzen
- Mobile Endgeräte überprüfen und gegen Diebstahl absichern
- Bei Verlust digitaler Datenträger oder mobilen Endgeräte dem Administrator bzw. Datenschutzbeauftragten melden
- Bei Auffinden von mobilen Speichergeräten z.B. USB-Sticks, Festplatten etc. an den zuständigen Administrator geben und nicht selbst untersuchen

Grundsätzlich bei der Nutzung von Computersystemen gilt, die Achtsamkeit sollte im Vordergrund stehen. Bei Vermutungen eines Sicherheitsverstoßes oder Fragen sollte sich immer an den zuständigen Administrator gewendet werden.

2.2.3 Passwortrichtlinie

Passwörter sind in der heutigen Zeit die am meist verwendete und einfachste Authentifizierungsmethode bei Anmeldungen an Systemen. Einfache Methoden bürgen jedoch auch die meisten Gefahren. Als Alternative gibt es mittlerweile verschiedene Methoden, die in Wissen (z.B. Passwort, PIN), Besitz (z.B. Chipkarte, TAN) oder Biometrie (z.B. Fingerabdruck, Gesichtserkennung) eingeteilt werden können. Oft werden Methoden auch kombiniert und ergeben zum Beispiel eine sicherere Zwei-Faktor-Authentisierung.[19]

Da in den meisten Fällen eine Anmeldung durch die reine Eingabe von Wissen geschieht, muss diese Methode besonders geschützt werden. Sichere Passwörter sind

[19] [BSI] Vgl. Zwei-Faktor-Authentisierung für höhere Sicherheit [online]

lang, bestehen aus Zahlen, Wörtern und Sonderzeichen. Unsichere und kurze Passwörter können schnell erraten (z.B. Brute-Force-Methode, Angriff durch reine Gewalt durch Erraten, Passwortlisten) werden. Auch persönliche Passwörter, wie Nachname, Alter, Firmenname, etc. sollten vermieden werden.

Im Falle eines bereits erfolgreichen Angriffes bzw. Bekanntmachung des Passwortes, werden Zugangsdaten meist in Passwortlisten gespeichert. Daher sollten bei verschiedenen Systemen und Webseiten auch verschiedene Passwörter verwendet werden. Eine gute Methode um festzustellen, ob sich jemand auf einer veröffentlichten Liste befindet ist das Angebot von Troy Hunt, (Microsoft Regional Direktor), welcher die Plattform „haveibeenpwned“[20] geschaffen hat und frei zur Verfügung stellt.

2.2.4 Datenschutzkonformes Verhalten

Ein datenschutzkonformes Verhalten im Unternehmen beschreibt Selbstverständlichkeiten und Verhaltensregeln, um den Schutz vertraulicher Informationen zu erhöhen. Der Mensch ist in der Kette, der Informationssicherheit, einer der größten Sicherheitslücken. Oft werden kleine Verhaltensregeln vergessen, in Folge dessen können Dokumente verschwinden, betriebsfremde Personen befinden sich unbeaufsichtigt im Gebäude oder vertrauliche Informationen gelangen an unbefugte Dritte. Im Folgenden werden einige Verhaltensregeln aufgelistet, welche die Sicherheit im Unternehmen bereits drastisch erhöhen können:

- Eine Einweisung aller Mitarbeiter und aller neuen Arbeitsplätze bzw. Hard- und Software sollte erfolgen und protokolliert werden.
- Besucher in den Gebäuden müssen immer beaufsichtigt und begleitet werden.
- Keine persönlichen Informationen z.B. am Telefon herausgeben.
- Geheime und Vertrauliche Dokumente nicht offen liegen lassen.
- Dokumente immer sicher vernichten.
- Passwortregelungen verwenden.
- Mobile Geräte und Schlüssel verschlossen aufbewahren oder am Körper tragen.
- Berufliche und Private Mails trennen und Anhänge auf Viren überprüfen.
- Die Nutzung des Internetzugangs beschränken.
- Nur sichere Kommunikationsmittel benutzen.
- Clean-Desk-Policy benutzen. Die Clean-Desk-Policy bezeichnet eine Verhaltensregel indem der Arbeitsplatz so verlassen wird, dass am nächsten Tag ein anderer Beschäftigter oder auch Fremder arbeiten kann ohne auf persönliche Dinge zu stoßen.

[20] [HIP] haveibeenpwned [online]

2.2.5 Beschäftigtendatenschutz

Je nach Abteilung fallen unterschiedliche Information und teils personenbezogene Daten an. Daher ist es notwendig neben der Grundschulung für den Datenschutz sich auch die speziellen Bedingungen in den jeweiligen Abteilungen anzuschauen und entsprechend zu handeln. Beschäftigte zählen zu den natürlichen Personen und haben gegenüber ihrem Arbeitgeber ebenfalls Rechte um ihre eigenen personenbezogene Daten zu schützen. Für ein Beschäftigungsverhältnis sind viele Informationen notwendig, jedoch muss nicht jeder Erhebung von persönlichen Daten zugestimmt werden.

Die meisten Informationen über Beschäftigte werden in der Personal- und Lohnbuchabteilung verarbeitet, diese sind in der Regel notwendige Daten für das Arbeitsverhältnis. Daten über schlechte Leistungen, Nichtleistungen oder konkrete Krankheitsgründe von Arbeitnehmer dürfen nicht gespeichert werden. Ausnahmen bilden hier beispielsweise Abmahnungen oder Verletzungen von Verstoßen.

Beim Recruiting gelten spezifische Regelungen. Allgemeine Intelligenz- oder Persönlichkeitstest dürfen für gewöhnlich nicht durchgeführt werden. Leistungstests, Arbeitsproben, Assessments müssen nachweislich geeignet und erforderlich sein. Grundsätzlich muss es sich um einen wissenschaftlich anerkannten Test, der durch fachkundiges Personal ausgeführt wird, handeln. Auch Bewerbungsdaten dürfen nur bei einem Arbeitsverhältnis oder einer Einwilligung für einen längeren Zeitraum gespeichert werden.

In einer Marketingabteilung müssen Regelung speziell für das Marketing beachtet werden. Es dürfen zum Beispiel keine Bilder von Beschäftigten, ohne Einwilligung, veröffentlicht werden, öffentliche Firmenkontaktdaten hingegen schon. Auch bei der Kundenakquise muss drauf geachtet werden nicht gegen gelten Regelungen zu verstoßen.

Bei der Sicherheitsabteilung bzw. in den eigenen Räumen des Arbeitgebers gelten strenge Vorgaben. Der Arbeitgeber darf sein eigenes Gut schützen, muss aber auf den Datenschutz der Mitarbeiter achten. Somit sind Videoüberwachungen nur unter bestimmten Umständen und nicht für die dauerhafte Überwachung von Personen gestattet. Zutrittsberechtigungen dürfen nicht zur Kontrolle missbraucht werden und die Ortung von beispielsweise Automobilen oder mobilen Endgeräten ist nur in bestimmten Einzelfällen erlaubt.

Dies waren nur einige Beispiele für spezifische Regelungen der einzelnen Abteilungen. Weitere Abteilungen wie das Lager, die Fertigung, die Qualitätssicherung, etc. müssen eigene Regelungen beachten und separat überprüft werden.[21]

[21] [SDS] Vgl. Beschäftigtendatenschutz [online]

2.2.6 Verhalten bei Datenpannen

Kommt es zu einer Sicherheitsverletzung bzw. Datenpanne, sollte schnell reagiert werden. „Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, dieser der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.“[22] Von der Entdeckung eines Sicherheitsverstoßes bis zur Übermittlung an den Vorgesetzen, Verantwortlichen und Datenschutzbeauftragten, welche die notwendigen Formalitäten erledigen, ist der Zeitraum sehr eng. Gegebenenfalls müssen auch die Betroffenen direkt kontaktiert werden.

Jede Sicherheitsverletzung sollte an den Verantwortlichen weitergeleitet werden, es kann lediglich im Einzelfall entschieden werden, ob ein Verstoß meldepflichtig ist oder nicht. Beispiele für meldepflichtige Vorfällen sind die Preisgabe von Kunden oder Mitarbeiterdaten, Verlust von mobilen Datenträger oder Systemen mit sensiblen Daten, Diebstahl oder auch der Angriff auf Kunden-, Mitarbeiter-, oder Mitgliedsdatenbanken.

„Mögliche Vorgehensweise bei einer Datenpanne:

1. **Datenschutzvergehen erkennen und schnell handeln:**
   Weiterleitung des Vorfalls vom Mitarbeiter an den Vorgesetzen, den Datenschutzkoordinator oder direkt an den Verantwortlichen für den Datenschutz.
2. **Bewertung:**
   Durchführung einer Risikoanalyse durch den Verantwortlichen für Datenschutz, um das Ausmaß abschätzen zu können.
3. **Maßnahmen zur Abwendung / Eindämmung:**
   Maßnahmen ergreifen, um gegen das Datenleck vorzugehen.
4. **Entscheidung, ob eine Meldung erfolgen soll:**
   Anhand der Bewertung entscheidet der Verantwortliche für Datenschutz, ob eine Meldung bei der Behörde erfolgen soll und ob Betroffene in Kenntnis gesetzt werden müssen.
5. **Meldung an die Aufsichtsbehörde oder / und an die Betroffenen:**
   Der Verantwortliche für Datenschutz erstattet Meldung bei der zuständigen Behörde.“[23]

[22] [DSGVO] § 33 Abs. 1

[23] [PPD] Datenschutz Schulung für Mitarbeiter, S.41

3 Konzeption des E-Learning Systems

Das folgende Kapitel gibt einen Überblick über die im Rahmen der Durchführung des Projektes verwendeten Techniken, welche als Grundlagen der Entwicklung dienen und die verwendeten Hilfsmittel, welche für die Konzeption des Systems zur Verfügung standen und genutzt wurden. Weiterhin werden Alternativen gezeigt, welche gegebenenfalls auch verwendetet werden können.

Im ersten Unterkapitel zu 3.1 wird die Technik erläutert, die für die Entwicklung des Systems genutzt wurde. Da die Software zur freien Verfügung im Internet stehen soll, ist es notwendig sich mit Themen wie Domainname, Web- und Datenbankserver zu beschäftigten. Unter diesen Aspekten werden auch die Programmiersprachen für das Back-End und das Framework für das Front- End ausgewählt.

Das zweite Unterkapitel zu 3.2 beschreibt die verwendeten Hilfsmittel, welche zur Verwirklichung des Projektes zur Verfügung standen und genutzt wurden. Im Rahmen des Projektes wurden, neben handschriftlichen Notizen und Skizzen, auf verschiedene Softwaresysteme zurückgegriffen, welche zur Unterstützung für Entwicklung, Design, Planung und Tests dienen.

3.1 Verwendete Technik

3.1.1 Hosting

Als webbasierte Anwendung muss entschieden werden, wie bzw. mit welchem Namen auf das System zugegriffen wird und wo dieses sicher abgelegt werden kann. In Anlehnung an die Datenschutz-Grundverordnung wird vorher festgelegt, dass das System in Deutschland gehostet wird.

Um das System im Internet aufzufinden muss mindestens ein Domainname registriert werden. Als erster Ansprechpartner für Domains in Deutschland steht die *DENIC eG*[24] zur Verfügung. Ihre Aufgabe ist die Verwaltung und der Betrieb der Top-Level-Domain .de. Zusätzlich kann auf der Webseite der *DENIC eG* bereits eine Verfügbarkeit des Namens überprüft werden. Domainregistrierungen sind bei unzähligen großen und kleinen Internet-Providern wie *1&1 Ionos SE*[25], *DENIC eG, Strato AG*[26], *Host Europe Limited*[27], *Hetzner Online GmbH*[28], u.a. möglich. Aus bereits positiven Erfahrung wurde der Anbieter *united-domains AG*[29] mit Sitz in Starnberg ausgewählt. In Folge dessen konnte der

[24] [FDE] Denic eG [online]

[25] [FIO] 1&1 Ionos SE [online]

[26] [FST] Strato AG [online]

[27] [FHE] Host Europe Limited [online]

[28] [FHO] Hetzner Online GmbH [online]

[29] [FUD] united-domains AG [online]

Hauptdomainname „elearningdatenschutz“ und ein Weiterleitungsname „elearningdsgvo“ mit der Top-Level-Domain .de registriert werden.

Nachdem entschieden wurde, wo die Domain registriert wird, muss noch ein sicherer Ablageort bzw. Webspace gefunden werden. Auf Grund der Tatsache, dass der Betrieb eines eigenen Webserver nicht notwendig ist , wurde mir der Webspace von der Firma *Mammut-Partner UG*[30] kostenfrei zur Verfügung gestellt. Der Server ist ein dedizierter Linux Server, welcher sich im Datacenter der Firma *Hetzner Online GmbH* in Nürnberg[31] befindet und ausschließlich für einen Betreiber zur Verfügung steht. Ein Auftragsverarbeitungsvertrag für das Hosting wurde abgeschlossen.

Weiterhin wird die Webanwendung noch mit einem Zertifikat versehen, um sichere HTTPS Verbindungen über Port 443 zu ermöglichen. Der Austeller des Zertifikates ist „Let´s Encrypt, eine freie, automatisierte und offene Zertifzierungsstelle“[32]

3.1.2 Webserver

Aufgrund des Hostings des Servers, stehen als Webserversoftware nur die Open Source Lösungen *NGINX*[33] und *Apache*[34] zur Verfügung. Beide Lösungen sind gut und zahlreich in Internet und Literatur dokumentiert. Apache ist schon länger im Markt und sticht mit seiner Flexibilität heraus, die Performance und Auslastung ist jedoch geringer. NGINX hebt sich in Performance und Auslastung bei statischen Anfragen hervor, kann aber keine dynamischen Inhalte ausliefern. Als Endlösung bietet es sich daher an, ein Zusammenspiel aus beiden Varianten zu verwenden.

In der folgenden Abbildung (Abbildung 1: Kombination aus Apache und NGNIX als Proxy) wird erläutert wie ein mögliches Szenario beider Lösungen funktioniert:

[30] [FMM] Mammut-Partner UG [online]

[31] [FHO] Hetzner Online GmbH [online]

[32] [LET] Let´s Encrypt [online]

[33] [WNX] NGINX [online]

[34] [WAP] Apache [online]

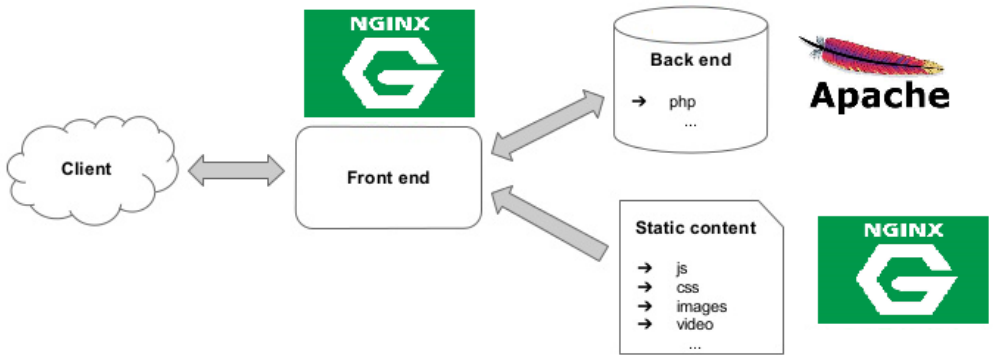

Abbildung 1: Kombination aus Apache und NGNIX als Proxy[35]

Anfragen laufen vom Client über NGINX als Reverse Proxy ein und statische Anfragen werden direkt von NGINX bearbeitet. Dynamische Aufgaben leitet NGINX an Apache weiter. Somit können die Vorteile aus beiden Lösungen kombiniert werden.

3.1.3 Programmiersprachen

Eine webbasierte Anwendung benötigt neben Auszeichnungssprachen auch logische Programmiersprachen.

Im Back-End wird *PHP*[36] in der derzeit aktuellen Version 7.4 genutzt. Als eine der ältesten und meist genutzten Programmiersprachen ist PHP sehr gut dokumentiert und enthält viele unterschiedliche Funktionen und Bibliotheken. Aktuelle beliebte Alternativen sind die performancestarke Sprache *Ruby*[37] oder die leichte Sprache *Python*[38].

Zur Anzeige von dynamischen Inhalten wird im Front-End *Javascript*[39] benutzt. Javascript ist neben PHP bei der Webprogrammierung eine klassische Wahl. Dessen ungeachtet basieren aktuell genutzte Bibliotheken wie *NodeJS*[40] und *React*[41] auf Javascript. Javascript ist genau wie PHP bereits längere Zeit am Markt und bietet sehr gute Dokumentationen und Performance. Aus diesem Grund wird auf die Nutzung einer anderen Sprache verzichtet.

[35] [WAX] Apache und NGINX [online]

[36] [LPH] PHP [online]

[37] [LRY] Ruby [online]

[38] [LPN] Python [online]

[39] [LJS] Javascript [online]

[40] [LNS] NodeJS [online]

[41] [LRT] React [online]

3.1.4 Datenbank

Zur persistenten Speicherung von Information wie Nutzerdaten oder Prüfungsergebnissen wird für das E-Learning System ein sicheres Datenbankmanagementsystem benötigt. Zur Auswahl stehen das klassische *MySQL*, die freie *MariaDB* und das kommerzielle *Oracle SQL*. Alle drei Datenbanksysteme sind gut und zahlreich in Internet und Literatur dokumentiert. Aus Kostengründen wird auf Oracle SQL verzichtet. MariaDB sticht im Vergleich zu MySQL besonders hervor durch seine Unabhängigkeit und die stetigen Weiterentwicklungen. Auf Grund dessen wird sich für den Einsatz des freien, relationalen Open-Source-Datenbankmanagementsystem MariaDB entschieden. [42]

3.1.5 UIKit

Um die Nutzungsfreundlichkeit zu erhöhen und das System responsiv auf mehreren Gerätearten nutzen zu können, wird zusätzlich für das Front-End das Framework *UIKIT* in Version 3.5 eingesetzt. „UIkit ist die Open-Source-Lösung zur Frontend-Programmierung der in Hamburg beheimateten Firma *YOOtheme*. Die umfangreiche Sammlung aus HTML-, CSS- und JavaScript-Komponenten untersteht der freien MIT-Lizenz und kann daher bedenkenlos genutzt und verändert werden. Die Core-Module bauen auf Normalize.css auf, weshalb gängige Internetbrowser keinerlei Probleme bei der Darstellung von UIkit-Webprojekten haben.

Alternativen die für UIKIT eingesetzt werden könnten, sind das meistgenutzte *Bootstrap* oder kleinere Frameworks, wie *Bulma*.“[43]

3.2 Verwendete Hilfsmittel

3.2.1 Visual Studio

Für die Entwicklung des Quelltextes kommt die integrierte Entwicklungsebene *Visual Studio*[44] von der Firma *Microsoft* zum Einsatz. Die IDE unterstützt die Softwareentwicklung mit diversen Funktionen wie Syntaxhervorhebung, Syntaxüberprüfungen, Online-Hilfen und automatischen Funktionserkennungen. Programmiersprachen werden analysiert und von der Software automatisch erkannt. Neben den bereits vorhandenen Sprachen können auch Erweiterungen für beispielsweise UIKit installiert werden. Insgesamt bringt Visual Studio alles mit, was zur Softwareentwicklung benötigt wird.

3.2.2 Plesk

Zur vereinfachten Verwaltung des Servers wird vom Hoster die Webserver-Distribution *Plesk*[45] eingesetzt. Plesk stellt dem Nutzer eine grafische Oberfläche für verschiedenste Aufgaben des Servers bereit. Praktisch alle wichtigen Vorgänge, wie die Verwaltung der

[42] [DMD] Vgl. MySQL und MariaDB Kap. 1.2 S.6-9

[43] [FUI] Vergleich von Frontend Frameworks [online]

[44] [SVS] Visual Studio [online]

[45] [SPK] Plesk [online]

Domain, die Erstellung von Datenbanken, das Einrichten eines Mailservers oder die Auswertung von Nutzungsstatistiken können über die Distribution leicht konfiguriert werden.

3.2.3 phpMyAdmin

Angesichts der Entscheidung, eine datenbankbasierte Anwendung zu erstellen, liegt es nahe, die Webanwendung *phpMyAdmin* zu verwenden. phpMyadmin ist die führende Open-Source-Anwendung zur Verwaltung von MySQL Datenbanken. Durch die Software lassen sich leicht Funktionen ausführen, wie Tabellen erstellen/verwalten, Datensätze bearbeiten oder Benutzerrechte verwalten, ohne selbst SQL-Befehle zu schreiben.[46]

3.2.4 Inkscape

Parallel zu textlichen Erläuterungen der Schulungsthemen werden zur Unterstützung Grafiken genutzt und erstellt. Dementsprechend müssen sich die Bilder flexibel den verschiedenen Geräten anpassen. Im Internet hat es sich bewährt auf Vektorgrafiken zu setzen. Vorteile sind die unbegrenzte Skalierbarkeit ohne Qualitätsverlust und mit einer geringen Speicher- bzw. Ladekapazität. Im Gegensatz zu Pixelbilder, setzen sich Vektorgrafiken aus mathematischen Formeln zusammen.

„Inkscape ist die kostenlose OpenSource-Variante für Vektorgrafiken. Inkscape ist das am weitesten verbreitete Open-Source-Programm für Vektorgrafiken. Es bietet eine gute Möglichkeit, in das Vektorzeichnen einzusteigen, und ist in vielen Bereichen eine interessante Alternative zu den kommerziellen Programmen.“ [47]

[46] [SPA] Vgl. Was ist phpMyadmin, S. 7-8

[47] [SIK] Inkscape, Kap 2, S.5

4 Prototypische Entwicklung des E-Learning Systems

Nachdem die Themen für die Schulung und die technischen Aspekte, sowie die Hilfsmittel ausgewählt wurden, kann die prototypische Entwicklung des Systems erfolgen.

Das folgende Kapitel gibt einen Überblick über des im Rahmen der Entwicklung des Projektes erzeugten Back-Ends, welches als Grundlagen für die Funktionen und den Aufbau des Systems dienen und das designen des Front-Ends, welche für die Nutzerinteraktion wichtig ist.

Im ersten Unterkapitel zu 4.1 wird das Back-End erläutert. Dementsprechend werden zuerst die Funktionen mit den jeweiligen Bibliotheken und Hilfsmittel bestimmt. Folglich lässt sich ein vorläufiges Datenbankdesign ableiten und bereits ein erster erweiterbarer Fragenkatalog erstellen.

Das zweite Unterkapitel zu 4.2 beschreibt das Design, die Entscheidungen und den Aufbau des Front-Ends. Ein User-Management muss aufgebaut und die Schulungsebene mit ihren Inhalten gefüllt werden. Weiterhin wird eine Prüfungsebene zur Ablegung einer Online-Prüfung erstellt. In Folge dessen muss eine Auswertung der abgelegten Prüfung und eine entsprechende Zertifizierung erfolgen.

Als weiteres werden im Unterkapitel zu 4.3 die vorgenommenen Tests, sowie ein Probekonto zur Verfügung gestellt.

Im letzten Unterkapitel zu 4.4 erfolgt schlussendlich eine Dokumentation der Aufwände und Kosten, welche für die Projektdurchführung aufgebracht wurden.

4.1 Back-End

4.1.1 Funktionen

Bei genauer Betrachtung der Anwendung (Abbildung 2: UML-Anwendungsfalldiagramm zur Funktionsbeschreibung) können die Funktionen in Nutzerfunktionen und Systemfunktionen unterschieden werden. Nutzerfunktionen beschreiben in erster Linie die Verarbeitung eigener personenbezogener Daten wie die Benutzererstellung, Verwaltung oder Änderung. Systemfunktionen hingegen sind systemspezifische Fälle wie zeitlich begrenzte Nutzung oder die allgemeine Verwaltung der bereitgestellten Angebote.

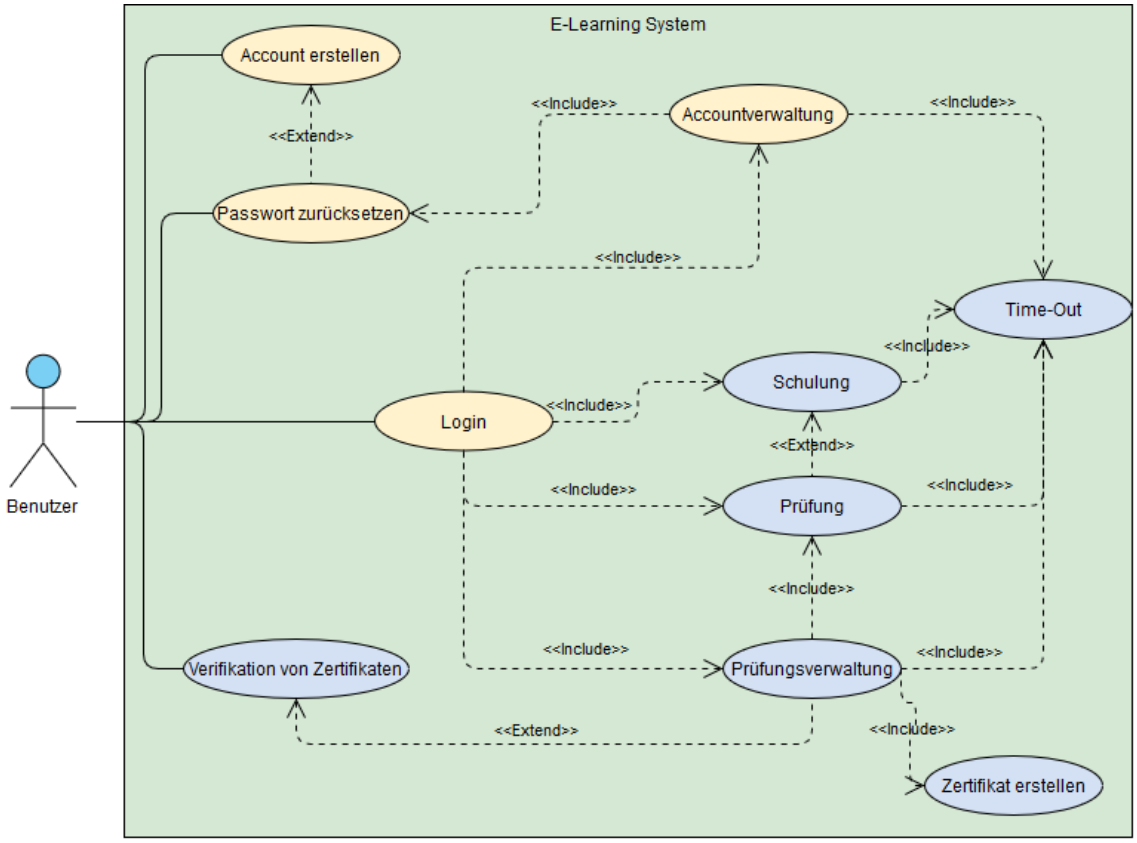

Abbildung 2: UML-Anwendungsfalldiagramm zur Funktionsbeschreibung

4.1.1.1 Nutzerfunktionen

Zur Nutzung des Angebotes müssen personenbezogen Daten verarbeitet werden. Personen müssen eindeutig identifizierbar sein, um später gegebenenfalls eine Zertifizierung zu erhalten.

Zuerst wird eine Benutzererstellung in Form eines Formulars angeboten. Aufgrund der eindeutigen Identifizierung sind Informationen wie Vor- & Nachname, Geburtsdatum, Geburtsort und E-Mailadresse notwendig und können durch die eigenen HTML Funktion *required* eingefordert und die Richtigkeit der angegebenen Daten durch die HTML-Funktion *pattern* eingeschränkt werden. Zum Schutz vor Missbrauch des Systems oder der persönlichen Daten wird zusätzlich ein *Captcha-Code*[48] und die PHP eigene Funktion *hash* mit dem Algorithmus *sha512* für die Passwortspeicherung verwendet. Die Daten werden zentral in einer Datenbank gespeichert.

Eine weitere Funktionalität stellt die Funktion *Passwort vergessen* dar. Über die Eingabe der Emailadresse lässt sich der Nutzer auffinden. Um unbefugten Eingriff zu verhindern, wird ein Token mit einer Gültigkeit von 24 Stunden generiert. Via der PHP eigenen Funktion *PHPMailer* wird dem Benutzer ein Zugrifflink gesendet, welcher den Token als GET Parameter übergibt. Durch den GET-Parameter wird der Token auf Gültigkeit überprüft und der Benutzer kann eigenständig das Passwort ändern.

[48] [CAP] Eigenes Captcha mit PHP [online]

Neben den beiden Funktionen zum Anlegen von Benutzerdaten, wird eine Login Funktion entwickelt. Ein Formular fragt E-Mailadresse und Passwort ab. Das Passwort wird in sha512 umgewandelt und mit dem Passwort in der Datenbank verglichen. Bei erfolgreichem Vergleich, wird mittels der PHP-Funktion *header* auf den privaten Bereich weitergeleitet und eine Session-Variable erstellt.

Bereits eingeloggte Benutzer können ihre Daten in einer Accountverwaltung anpassen. Da es untypisch ist, Daten wie Name oder Geburtsdatum zu ändern, sind die Felder im entsprechenden Formular mit der HTML eigenen Funktionen *disabled* ausgegraut und werden nicht übergeben. Nur die Daten Firma und Passwort können geändert werden. Bei generellen Fehlern können Benutzer den Umweg über E-Mail gehen und die Daten werden direkt in der Datenbank angepasst.

Allgemeine Fehlerabfragen werden mittels PHP-Funktionen wie isset oder if abgefangen und entsprechende Meldungen über die JS-Funktion *alert* ausgegeben.

4.1.1.2 Systemfunktionen

Das E-Learning System benötigt einige systemrelevante Funktionen. Speziellere Funktionen umfassen das Angebot der Schulung, automatische Timeouts, die Abfrage des Wissens oder auch die Erstellung des Zertifikats.

Zur allgemeinen Sicherheit im privaten Bereich trägt eine Timeout-Funktion bei, welche auf jeder abgerufenen Seite abfragt, ob einem Benutzer eine Session-Variable zugewiesen ist. Weiterhin speichert die Funktion die Zugriffzeit auf der jeweiligen Seite und zerstört nach Ablauf von 20 Minuten die Session automatisch. Sollte einer der beiden Fälle eintreten, wird der Benutzer aus dem privaten Bereich entfernt und auf eine Mitteilungsseite weitergeleitet.

Um für die Schulungsinhalte nicht immer neue Seiten zu erstellen, werden diese zentral gefasst und mit Kapitelnummern versehen. Die Funktion GET ruft im Schulungsbereich die Kapitel ab und stellt diese grafisch dar.

Eine der wichtigsten Funktionen ist die Abfrage des Wissens. Die Prüfung ruft nach Kapitel sortiert eine zufällige in der Datenbank abgelegte Frage mittels SQL Befehl *order by rand* und *limit 1* auf inkl. der dazugehörigen passenden Antworten. Mit einem Formular aus Checkboxen kann der Benutzer seine Antworten abgeben. Nach Abgabe werden die vom Benutzer abgegebenen Antworten mit den richtigen Antworten aus der Datenbank verglichen. Bei richtiger Antwort wird eine Variable hochgezählt, bei falscher abgezogen. Am Ende der Prüfung werden die maximal erreichbaren und erlangten Punkte verrechnet und in der Datenbank als Versuch gespeichert. Bei Erreichen von mehr als 50% gilt die Prüfung als bestanden und wird mit einem Verifikationscode versehen.

Die Prüfungsverwaltung beinhaltet eine Zusammenfassung aller getätigten bestandener und nicht bestandener Prüfungen. Nach Datum und Uhrzeit sortiert, erhalten Benutzer einen prozentualen Überblick aller eigenen Ergebnisse aus der Datenbank. Bei Erreichen von mindestens 50% steht eine Schaltfläche zur Erstellung eines Zertifikats zur

Verfügung. Bei Nichtbestehen ist die Schaltfläche durch die HTML Funktion *disabled* ausgegraut und nicht anwählbar.

Zur Erstellung eines Zertifikats wird die PHP-Bibliothek *TCPDF*[49] verwendet. *TCPDF* ist eine kostenlose Bibliothek zur Erstellung von PDF-Dokumenten. Mittels *SQL JOINS* werden alle notwendigen Datensätze aus der Datenbank kombiniert und den entsprechenden Variablen zugewiesen. Durch das Übersetzen von HTML-Code wird das PDF erstellt und direkt durch den Browser an den Benutzer gesendet.

Um die Gültigkeit der Zertifikate zu überprüfen steht eine Verifikationsfunktion zur Verfügung. Durch den zufallsgenerierten Verifikationscode bei bestandener Prüfung können auch nicht registrierte Benutzer mittels Formular die Gültigkeit überprüfen. Mittels Datenbankabfrage wird der eingegebene Code verglichen und durch die JS-Funktion *alert* eine Rückmeldung gegeben.

4.1.2 Datenbankdesign

Das E-Learning System verwaltet Benutzer, Fragen, Antworten und Prüfungsergebnisse in einer MariaDB Datenbank. Das folgende Entity Relationship Diagramm (Abbildung 3: Entity Relationship Diagramm des E-Learning Systems) gibt die Tabellen und ihre Beziehungen zueinander an.

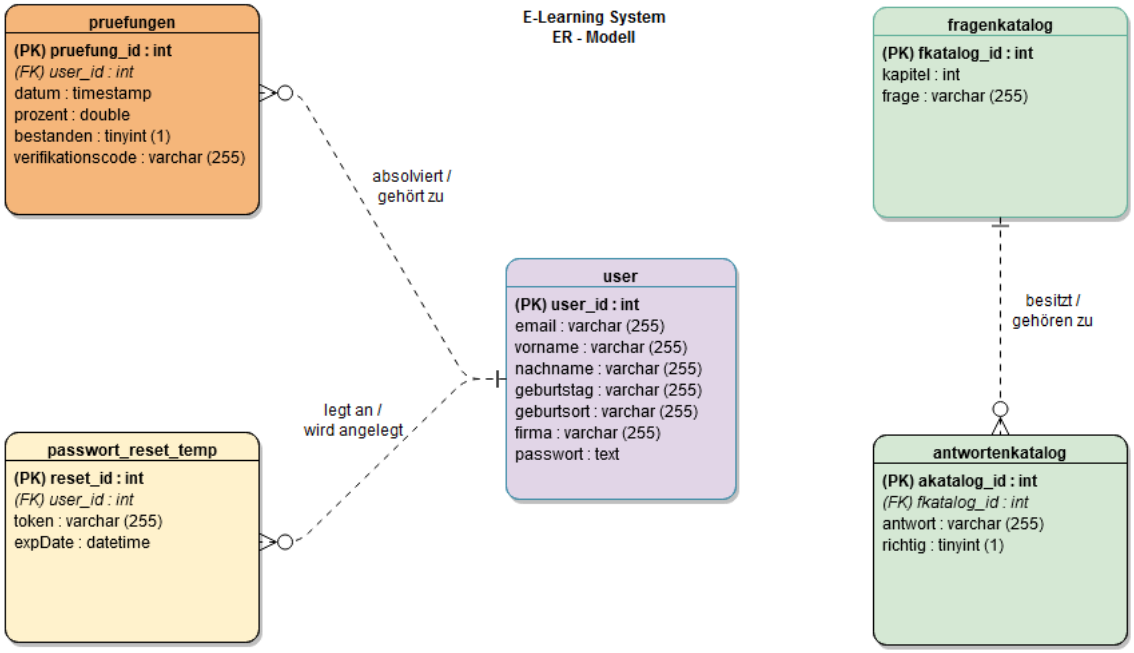

Abbildung 3: Entity Relationship Diagramm des E-Learning Systems

User: Die Tabelle *User* enthält Stammdaten aller registrierten Benutzer des E-Learning Systems. Die Daten werden hauptsächlich zur Authentifizierung, sowie zur Erstellung des zu erreichenden Zertifikats genutzt. Als Primärschlüssel wird jedem Benutzer automatisch eine *user_id* angelegt, diese gilt zugleich als Kundennummer. Die Daten für

[49] [TCP] TCPDF [online]

email und *passwort* werden für die Authentifizierung am System benötigt. Die Informationen *vorname*, *nachname*, *geburtstag*, *geburtsort* sind zur eindeutigen Identifizierung einer Person und deren Zertifizierung vorgesehen. Aufgrund der Notwendigkeit, sind diese Felder Pflichtfelder. Die Information *firma* ist freiwillig und wird grundsätzlich nicht benötigt, kann aber als erleichterter Suchindex verwendet werden.

Pruefungen: Die Tabelle *Pruefungen* enthält alle Ergebnisse über bestandene und nichtbestandene Prüfungen der Benutzer. Als Primärschlüssel wird zu jeder Prüfung automatisch eine *pruefung_id* vergeben. Zur eindeutigen Zuweisung der Benutzer ist der Fremdschlüssel *user_id* eingetragen. Die Tabellen *pruefungen* und *user* stehen in einer 0-n:1 Beziehung. Ein Benutzer absolviert mehrere Prüfungen und mehrere Prüfungen gehören zu einem Benutzer. Das Feld *datum* enthält einen automatisch erzeugten Zeitstempel vom Server beim Erzeugen des Datensatzes und wird als Nachweiszeitpunkt verwendet. Die Felder *prozent* und *bestanden* enthalten Informationen über das Ergebnis der Prüfung. *prozent* enthält den genauen Prozentsatz über das Ergebnis und *bestanden* wird als Boolean eingesetzt um das Bestehen bzw. Nichtbestehen zu dokumentieren. Das Feld *verifikationscode* wird bei erfolgreicher Prüfung durch eine PHP-Funktion mit einem zufällig erzeugten Code versehen und dient der späteren Verifikation der Zertifikate.

Passwort_reset_temp: Die Tabelle passwort_reset_temp dient ausschließlich der Zurücksetzung von Benutzerpasswörtern. Als Primärschlüssel wird zu jeder Anfrage automatisch eine *reset_id* erstellt. Vergleichsweise mit der vorherigen Tabelle wird auch hier der Fremdschlüssel *user_id* vergeben. Die Tabellen *passwort_reset_temp* und *user* stehen in einer 0-n:1 Beziehung. Ein Benutzer kann mehrere Passwortzurücksetzungen durchführen und mehrere Passwortzurücksetzungen werden durch einen Benutzer angelegt. Das Feld *token* und *expDate* dienen zusammen als Sicherheitsmaßnahme. Bezugnehmend wird ein zufällig erzeugter Token vergeben, der im späteren Verlauf als GET Parameter genutzt wird. *expDate* ist ein ausgerechneter Zeitpunkt um die Gültigkeit zu gewährleisten. Aufgrund der Sicherheitsaspekte ist ein Datensatz immer nur 24 Stunden gültig und wird danach unbrauchbar.

Fragenkatalog: Die Tabelle *fragenkatalog* enthält alle möglichen Fragen, welche in der Prüfung abgefragt werden können. Hinsichtlich der eindeutigen Zuordnung von Fragen und Antworten wird der Primärschlüssel fkatalog_id automatisch erzeugt. Für die Indexierung zu ihren dazugehörigen Kapiteln und aufgrund der Tatsache, dass jedes Kapitel mindestens einmal in der Prüfung behandelt werden soll wird das Feld *kapitel* genutzt. Das Feld *frage* enthält die eigentliche Prüfungsfrage in Textform.

Antwortenkatalog: Die Tabelle *antwortenkatalog* dient der Zuordnung von möglichen richtigen, sowie falschen Antworten zu den Prüfungsfragen. Der Primärschlüssel *akatalog_id* wird jeder Antwort automatisch zugewiesen. Zur Zuordnung der Fragen zu den Antworten dient als Fremdschlüssel die *fkatalog_id*. Die Tabellen *antwortenkatalog* und *fragenkatalog* stehen in einer n:1 Beziehung. Eine Frage besitzt mehrere Antwortmöglichkeiten und mehrere Antworten gehören zu einer Frage. Das Feld *antwort* enthält die

eigentliche Antwort in Textform. Zur Differenzierung von richtigen und falschen Antworten enthält die Tabelle mit der Eigenschaft eines Boolean das Feld *richtig.*

4.1.3 Fragenkatalog

Aufgrund der Flexibilitätsmöglichkeiten der Prüfung, wird ein umfassender Fragenkatalog (Tabelle 4: Fragenkatalog) errichtet. Die Speicherung und Verwaltungen in einer Datenbank birgt viele Vorteile. Fragen können je nach Bedarf einfach ausgetauscht, neue hinzugefügt oder korrigiert werden. Derzeitig beinhaltet die Schulung 15 Kapitel und somit 15 notwendige Fragen in der Prüfung. Damit Teilnehmer nicht immer die gleichen Fragen erhalten, werden zu jedem Kapitel vier Fragen erstellt. Dem zufolge umfasst der Fragenkatalog insgesamt 60 Möglichkeiten. Mathematisch gesehen ist die Wahrscheinlichkeit die identische Prüfung ein zweites Mal durchzuführen 1 zu 1.073.741.824.

4.2 Front-End

4.2.1 Struktur und Design

Um genug Sicherheit zu bieten wird es einen eingeloggten Bereich(Abbildung 5: Startseite privater Bereich) für registrierte Benutzer und einen ausgeloggten Bereich(Abbildung 4: Startseite anonymer Bereich) für anonyme Benutzer geben. Im ausgeloggten Bereich können auf die Funktionen Account erstellen, Passwort vergessen, den Login und Verifikation von Zertifikaten zugegriffen werden. Der eingeloggte Bereich behandelt die restlichen Funktionen, wie Accountverwaltung, die eigentliche Schulung mit anschließender Prüfung und die Prüfungsverwaltung mit der Zertifikatsausstellung.

Die Navigation des Systems wird durch verschiedene Menüs vereinfacht. In normaler Desktopansicht wird ein Zusammenspiel aus Navigationsleisten und Listen eingesetzt. Auf mobiler Ebene werden diese Elemente aufgrund von Platzmangel vollständig entfernt und durch Off-Canvas-Technik ersetzt. Off-Canvas wird meist in responsiven Webseiten benutzt und verschiebt bestimmte Elemente aus dem Sichtfeld um auf kleineren Displays mehr Platz zu bieten.

Für die bessere Auffindbarkeit, stellt die Webseite Favoriten-Icons für diverse Endgeräte und Browser zur Verfügung. Favoriten-Icons sind kleine Grafiken, welche als Schnellstart-Symbol für die Webseite dienen. Aufgrund der Browser- und Betriebssystemunabhängigkeit müssen mehrere Dateien in unterschiedlichen Größen vorliegen. In diesem Falle wird das Logo der Webseite komprimiert und in fünf unterschiedlichen Formaten gesichert. Damit Systeme die Icons auffinden können, müssen diese direkt im Stammverzeichnis auffindbar sein.

4.2.2 Schichten

Das Front-End bzw. die Weboberfläche des Systems besteht im Wesentlichen aus 3 verschiedenen Schichten, welche jeweils in Abhängigkeit zueinander genutzt werden. Das User-Management unter 4.2.1.1 stellt den Kern eines jeden Systems dar, welche personenbezogene Daten verwendet oder Authentifizierung von Benutzern verlangt. Die

Schulungsebene zu 4.2.1.2 bezieht sich auf die Vermittlung von Informationen über die einzelnen Themengebiete. Am Ende steht die Prüfungsebene zu 4.2.1.3 welche für die Abfrage des zu erwartenden Wissens steht.

4.2.2.1 User Management

Das User Management als Kern des Systems umfasst die Abfrage der benötigten persönlichen Informationen für die Authentifizierung und Validierung von Benutzern. Über die Startseite stehen als Grundaufgaben die Funktionen Login, Benutzer Account erstellen und Passwort vergessen mittels grafischen Formularen zur Verfügung. Im eingeloggten Bereich steht dem Benutzer frei seine persönlichen Daten zum Teil zu korrigieren oder zu erneuern. Da es für einige Daten z.B. Geburtsdatum ungewöhnlich ist diese zu bearbeiten, sind diese Daten in den Formlaren gesperrt(Abbildung 6: Verwaltung persönlicher Daten). Bei fehlerhaften Eingaben wird der Benutzer durch verschiedenste Elemente benachrichtigt und zur Korrektur aufgefordert.

4.2.2.2 Schulungsebene

Um Benutzern das Lernen so angenehm wie möglich zu gestalten, wurde auf verschiedene Methoden zurückgegriffen. Visualisierung fördert allgemein das Verständnis und die Anwendung. Die Schulung(Abbildung 7: Datenschutzschulung) ist in verschiedene kleinere Kapitel unterteilt und das wichtigste zusammengefasst. Bei schwierig zu verstehenden Informationen wurden eine Assoziation mit Beispielen gebildet. Weiterhin enthalten die Kapitel unterschiedliche Grafiken mit den wichtigsten Punkten, Beispielen aus der Realität oder weiteren Studien.

4.2.2.3 Prüfungsebene

Die Prüfungsebene umfasst die Aufgabe der Abfrage des gelernten Wissens. Zuerst wird dem Prüfling der Ablauf und die Punktewertung wie folgt erläutert. Die Prüfung(Abbildung 8: Prüfungen) wird als Multiple Choice Prüfung angeboten. Es gibt immer mindestens eine richtige Antwort, es können aber auch alle Antworten richtig sein. Eine richtige Antwort gibt einen Punkt, eine falsche einen Punkt Abzug. Negative Punkte sind dadurch möglich. Die Fragen werden nach dem Zufallsprinzip ausgewählt und können im Wortlaut unterschiedlich sein. Es dürfen nur Bedienelemente des Systems und nicht vom Browser benutzt werden. Bezogen auf die unterschiedlichen Themen, gibt es zu jedem Kapitel genau eine Frage, welche durch das Lernmaterial immer beantwortet werden kann. Eine bestimmte Zeitvorgabe gibt es nicht. Um die Möglichkeit der Täuschung einzugrenzen, gibt jeder Benutzer vor der Prüfung noch eine Bestätigung zu einer Eigenständigkeitserklärung ab.

4.2.3 Zertifizierung

Bei bestandener Prüfung kann der Benutzer mittels Prüfungsverwaltung(Abbildung 9: Prüfungsverwaltung) ein Zertifikat erzeugen. Das Zertifikat(Abbildung 10: Zertifizierung) gilt als eigener persönlichen Nachweis und zur Erfüllung der Nachweispflicht bzw. der Dokumentationsplicht für den Arbeitgeber. Im Zertifikat enthalten sind unter anderem die

persönlichen Daten des Prüflings, das Prüfdatum, die vermittelten Kenntnisse und der Verifikationscode. Die Gültigkeit lässt sich einfach über die Startseite überprüfen. Zur regelmäßigen Auffrischung und auf dem neusten Stand zu bleiben, sollte das Zertifikat nicht älter als ein Jahr sein.

4.2.4 Rechtliche Aspekte

Öffentliche Systeme und Webangebote müssen sich an gewisse rechtliche Pflichten halten. In Übereinstimmung mit dem Telemediengesetz gilt eine Impressumspflicht. Aufgrund dessen sollte von jeder Seite direkt aufs Impressum zugegriffen werden können. Neben der Auskunftspflicht wird hier unter anderem auch die Haftung der Inhalte, Links, Nachweise und das Urheberrecht behandelt.

Neben dem Impressum muss laut Datenschutzgesetz auch eine Datenschutzerklärung vorliegen. In dieser Erklärung wird dem Benutzer unter anderem erläutert wer für die Datenverarbeitung zuständig ist, wie Daten erfasst werden, zu welchem Zweck und in welchem Umfang personenbezogenen Daten verarbeitet werden. Weiterhin werden die Rechte genannt, die gegenüber dem Webseitenbetreiber geltend gemacht werden können und einige technische Details zur Datensammlung. Aufgrund der notwendigen technischen Funktionalität und dem Wegfall von Datensammlungen zwecks Werbezwecken, kann sich eine Abfrage zur Akzeptierung von Cookies erübrigen.

Da diese Dokumente gegenüber der Aufsichtsbehörde und Mitbewerbern öffentlich einsehbar sind, bieten sie eine große Angriffsfläche und sollten sorgfältig überprüft und angelegt werden.

4.3 Testmöglichkeiten

Das System ist im Internet unter dem primären Domainnamen https://www.elearningdatenschutz.de/ oder der Weiterleitungsdomain https://www.elearningdsgvo.de/ aufrufbar. Zum einen kann ein kostenloser Account erstellt werden. Zum anderen steht ein Test-Account zur Verfügung, welcher in der Entwicklungsphase für verschiedene Tests (z.B. Prüfungsauswertungen, Umgang mit Umlauten, etc.) diente. Das Zurücksetzen bzw. die Änderung des Passwortes für den Benutzer wird durch Funktionen verhindert.

Kundennummer:	7
Vorname:	Mäx
Nachname:	Müstermann
Email:	max.mustermann@t-online.de
Kennwort:	test

Tabelle 2: Testmöglichkeit

4.4 Dokumentation der Aufwendungen

Bei der Durchführung des Projektes entstanden unterschiedliche Aufwände und Kosten. Einerseits mussten tiefergehende Kenntnisse im Bereich des Datenschutzes erlernt und

durch ein entsprechendes Zertifikat nachgewiesen werden. Anderseits entstanden durch die Planung und Entwicklung des E-Learning Systems verschiedene Kosten. Es wurde zwar drauf geachtet Open-Source Produkte zu nutzen, jedoch sollte bei einem dauerhaften Betrieb nicht an Kosten gespart werden. Im Folgenden befindet sich eine tabellarische Auflistung der Aufwendungen:

Position	Bezeichnung	Menge	Einzel	Gesamt
1	Datenschutz-schulung incl. Prüfungskosten	1	593,81 €	593,81 €
2	Fachliteratur Datenschutz	pauschal	230,24 €	230,24 €
3	Domainnamen	2, Jährlich	9,99 €	19,98 €
4	Hosting	/	0,00 €	0,00 €
5	Hard- & Software	/	0,00 €	0,00 €
Zwischensumme				844,03 €
6	Kalkulatorische Entwicklungskos-ten	240 h	90,00 €	21.600,00 €
Gesamt				**22.444,03 €**

Tabelle 3: Aufwendungen

5 Fazit

Das Ziel dieses Praxisprojektes war es ein E-Learning System zu entwickelt, welches als asynchrones und freies Online-Format die Datenschutzschulungen in Unternehmen verbessern kann. Die Durchführung des Projektes konnte weitgehend wie geplant realisiert werden und wurde bereits von verschiedenen Probanden getestet. Insgesamt schafft die Software eine gute Alternative zu einer kostspieligen Schulung und schafft somit einen Mehrwert für die Allgemeinheit. Das erforderliche Wissen kann gut vermittelt werden und die Abfrage zur Zertifizierung ist vom Schwierigkeitsgrad angemessen. Erst recht da Homeoffice immer beliebter und notwendiger wird, entfallen vermehrt Präsenzschulungen und Unterricht. In Folge dessen wird der Datenschutz im Unternehmen und im eigenen Heim noch stärker vernachlässigt. Als ein notwendiges und wichtiges Thema sollte jeder in der Lage sein, die erarbeiteten Schulungsthemen zu verstehen und anzuwenden. Eine Auffrischung oder die Einführung eines neuen Mitarbeiters kann durch die Software zu jeder Zeit realisiert werden. Weiterhin können bei einer Kontrolle der Aufsichtsbehörde die Zertifikate der Teilnehmer im Unternehmen vorgelegt werden.

Dank dem responsiven Design(Abbildung 11: Responsive Design 1 u. Abbildung 12: Responsive Design 2) ist es möglich von verschiedenen Geräten mit unterschiedlicher Bildschirmauflösung die Software aufzurufen und alle Funktionen auszuführen. Hierbei wird die Seite, sowie die Menüstrukturen automatisch angepasst und aktualisiert. Alle Funktionen funktionieren wie geplant und bei Eingabegehlern gibt die Software eine passende Fehlermeldung aus. Durch die Verwendung einer Datenbank konnten viele Funktionen automatisiert werden. Der Fragenkatalog ist beliebig erweiterbar und weitere Schulungsthemen lassen sich leicht hinzufügen.

Trotz der im allgemeinen positiv verlaufenden Realisierung, konnten einige sekundäre Punkte nicht wie geplant umgesetzt werden. Die in der Schulung enthaltenen Grafiken wurden teils durch passende fremde Grafiken ersetzt, da diese besser gestaltet waren und zum Thema passten. Für die Prüfung war ein Vollbildmodus vorgesehen, dieser konnte auf Computern gestartet, jedoch nicht beendet werden. Auch im Bereich der mobilen Geräte konnte dies nicht wie geplant realisiert werden. Weiterhin funktioniert zwar die Prüfung einwandfrei, allerdings gibt es keine Einsicht über die getätigten Fehler eines Einzelnen und eine Täuschung kann nicht erkannt werden.

Für die Zukunft des Projektes sind viele Erweiterungen und Verbesserungen geplant. Da das System für eine Schulung bereits steht, können weitere spezifische Anwenderschulungen und Prüfungen eingefügt werden. Auch die oben genannten Fehler können ausgebessert werden. Für die Schulung im Allgemeinen wäre auch denkbar einen synchronen Unterricht als ein Teil Präsenzveranstaltung und ein Teil Onlinekurs einzuführen.

Das System befasst sich im Allgemeinen nur mit der Schulung eines Einzelnen. Unternehmen können diese zwar nutzen, sollten aber bedenken, dass dies nur ein Teilbereich

des Datenschutzes darstellt. Weitere Aufgaben sind zur Erfüllung der Umsetzung im Unternehmen notwendig. Daher soll im Rahmen der Bachelorarbeit ein Leitfaden entstehen, wie Unternehmen den Datenschutz angehen und umsetzen können.

Literaturverzeichnis

[ADP] Aichinger, Matthias, Dolezal, Andreas, Datenschutz in der Praxis, myMorawa, Salzburg, 2018

[BDSG] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680(Datenschutz-Anpassungs- und -Umsetzungsgesetz EU–DSAnpUG-EU), Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 44, Bonn, 05. Juli 2017

[BFDI] Prof. Kelber, Ulrich, Winkler, Luca, Weick, Coletta, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, abgerufen am 30 Januar 2021 https://www.bfdi.bund.de/DE/Datenschutz/datenschutz-node.html, (o. D.)

[BSI] Bundesamt für Sicherheit in der Informationstechnik, Referat WG 25, Cyber-Sicherheit für den Bürger, abgerufen am 30 Januar 2021 von https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei-Faktor-Authentisierung_node.html, Bonn, (o. D.)

[CAP] Tristan Radtke, united-domains AG, abgerufen am 30 Januar 2021 von https://www-coding.de/so-gehts-eigenes-captcha-mit-php/, April 2019

[DMD] Adams, R., SQL: der Grundkurs für Ausbildung und Praxis: mit Beispielen in MySQL/MariaDB (2., aktualisierte Auflage). München: Hanser., 2016

[DSGVO] Europäische Union, Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union, Brüssel, 04. Mai 2016

[DSR] Unabhängig veröffentlicht, DatSchR Datenschutzrecht 3. Auflage 2019, Amazon Distribution GmbH, Leipzig, 2019

[FDE] Martin Küchenthal, Andreas Musielak, Sebastian Röthler, Dr. Jörg Schweiger, DENIC eG, abgerufen am 30 Januar 2021 von https://www.denic.de/, (o. D.)

[FHE] Dr. Christian Koch, Tim Montag, Jonathan Wong, Host Europe GmbH, abgerufen am 30 Januar 2021 von https://www.hosteurope.de/, (o. D.)

[FHO] Martin Hetzner, Stephan Konvickova, Günther Müller, Hetzner Online GmbH, abgerufen am 30 Januar 2021 von https://www.hetzner.de/, (o. D.)

[FIO] Hüseyin Dogan, Dr. Martin Endreß, Claudia Frese, Hans-Henning Kettler, Matthias Steinberg, Achim Weiß, 1&1 IONOS SE, abgerufen am 30 Januar 2021 von https://www.ionos.de, (o. D.)

[FMM] Michael Koszalsky, Mammut-Partner UG, abgerufen am 30 Januar 2021 von https://www.mammut-partner.de, (o. D.)

[FST] Hüseyin Dogan, Dr. Martin Endreß, Claudia Frese, Hans-Henning Kettler, Matthias Steinberg, Achim Weiß, STRATO AG, abgerufen am 30 Januar 2021 von https://www.strato.de/, (o. D.)

[FUD] Markus Eggensperger, Maximilian Burianek, Tobias Sattler, united-domains AG, abgerufen am 30 Januar 2021 von https://www.united-domains.de/, (o. D.)

[FUI] IONOS, abgerufen am 30 Januar 2021 von https://www.ionos.de/digitalguide/websites/web-entwicklung/bootstrap-fuenf-alternativen-zum-twitter-framework/, September 2020

[HIP] Hunt, Troy, Microsoft Regional Direktor, abgerufen am 30 Januar 2021 von https://haveibeenpwned.com/, (o. D.)

[ICS] intersoft consulting services AG, abgerufen am 30 Januar 2021 von https://www.datenschutzbeauftragter-info.de/datenschutz-grundverordnung-recht-maessigkeit-der-datenverarbeitung/, (o. D.)

[LDI] Block, Helga, Landesbeauftragte für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen, abgerufen am 30 Januar 2021 von https://www.ldi.nrw.de/mainmenu_Datenschutz/Inhalt/Datenschutz/Datenschutz.php, (o. D.)

[LET] Internet Security Research Group, Let´s Encrypt, abgerufen am 30 Januar 2021 von https://letsencrypt.org/de, (o. D.)

[LJS] MDN contributors, Cris Mills, Javascript, abgerufen am 30 Januar 2021 von https://developer.mozilla.org/en-US/docs/Web/JavaScript, August 2020

[LNS] OpenJS Foundation, NodeJS, abgerufen am 30 Januar 2021 von https://nodejs.org/de/, (o. D.)

[LPH] PHP Group, PHP, abgerufen am 30 Januar 2021 von https://www.php.net/, (o. D.)

[LPN] Python Software Foundation, Python, abgerufen am 30 Januar 2021 von https://www.python.org/, (o. D.)

[LRT] Facebook Inc., React, abgerufen am 30 Januar 2021 von https://reactjs.org/, (o. D.)

[LRY] Ruby-Community, Yukihiro Matsumoto, Ruby, abgerufen am 30 Januar 2021 von https://www.ruby-lang.org/de, (o. D.)

[OHF] Howanietz, Friedrich, Verarbeiter, abgerufen am 30 Januar 2021 von https://eu-datenschutz-grundverordnung.net/verarbeiter/, (o. D.)

[PPD] Petzka, Patrick, Datenschutz Schulung für Mitarbeiter, PETZKA VERLAG, Traunreut, 2018

[SDS] Prof. Dr. Riechert, Anne, M.A. Simon, Antje, Stiftung Datenschutz, Beschäftigtendatenschutz Handreichung, abgerufen am 30 Januar 2021 von https://stiftung-datenschutz.org/fileadmin/Redaktion/Beschaeftigtendatenschutz/SDS_Datenschutz_Beschaeftigte_2020-01-16.pdf, Juli 2018

[SIK] U. Schöler, Inkscape: professionelle Vektorgrafiken gestalten. München [u.a.], Addison-Wesley, 2010

[SKI] Schmidt, Klaus, Der IT Security Manager, Carl Hanser Verlag München Wien, 2006

[SPA] M. Delisle, Mastering phpMyAdmin 3.4 for effective MySQL management: a complete guide to getting started with phpMyAdmin 3.4 and mastering its features. Birmingham, Packt Pub., 2012.

[SPK] Plesk International GmbH, abgerufen am 30 Januar 2021 von https://www.plesk.com/, (o. D.)

[STB] Stapelkamp, Torsten, DSGVO-Bibel, Design is making Sense, Leipzig, 2018

[SVS] Microsoft, abgerufen am 30 Januar 2021 von https://visualstudio.microsoft.com/de/vs/, (o. D.)

[TCP] Nicola Asuni, abgerufen am 30 Januar 2021 von https://tcpdf.org/

[WAP] Apache Group, Apache, abgerufen am 30 Januar 2021 von https://httpd.apache.org/, (o. D.)

[WAX] Kasyanova, Alisa abgerufen am 30 Januar 2021 von https://support.plesk.com/hc/en-us/articles/360003248534-How-a-combination-of-Apache-and-nginx-in-proxy-mode-works-in-Plesk-for-Linux, Juni 2020

[WNX] F5 Networks Inc., NGINX, abgerufen am 30 Januar 2021 von https://www.nginx.com/, (o. D.)

Anhang

Kapitel	Frage
1	Benennen Sie fundamentale Themen im Datenschutz!
	Welche Wörter passen zum Datenschutz?
	Welche Ziele sollen in der Schulung erreicht werden?
	Welchen Nutzen hat eine Schulung zum Datenschutz?
2	Welche internationalen Datenschutzgesetze gibt es?
	In welchen nationalen Gesetzen befinden sich u.a. datenschutzrechtliche Aspekte?
	Was ist Datenschutz?
	Wofür wird Datenschutz benötigt?
3	Was schützt die DSGVO?
	Wer sind die zwei Hauptakteure im Datenschutz?
	Wann wird ein Datenschutzbeauftragter benötigt?
	Wann liegt eine Auftragsverarbeitung vor?
4	Welcher Begriff zählt nicht zur Gruppe von personenbezogener Daten?
	Welche dieser vier Punkte zählt nicht zu den sensiblen Daten?
	Was sind personenbezogene Daten?
	Was gilt bei der Verarbeitung von personenbezogenen Daten bei Kindern grundsätzlich?
5	Was gehört zu den Grundsätzen der Verarbeitung?
	Was gehört nicht zu den Grundsätzen der Verarbeitung?
	Bennen Sie die richtigen Beispiele für die Grundsätze der Verarbeitung
	Ist die Verarbeitung personenbezogener Daten grundsätzlich erlaubt?
6	Wann ist die Verarbeitung rechtmäßig?
	Wer darf Ihre persönlichen Daten grundsätzlich verarbeiten?
	Welche Rechtmäßigkeiten gibt es?
	Sie haben einen Autounfall, ihre Kontaktdaten werden ohne Einverständnis der Polizei übergeben, ist diese Verarbeitung rechtmäßig?
7	Welche Rechte haben Betroffene?
	Welche Frist wird dem Verantwortlichen bei der Auskunftspflicht vorgegeben?
	Müssen beim Recht auf Löschung alle Daten gelöscht werden?
	Darf eine Maschine alleine wichtige Entscheidungen über Sie treffen?
8	Welche Strafen können bei Verstößen gegen den Datenschutz erwartet werden?
	Unter welchen Umständen können Freiheitsstrafen bei Verstößen verhängt werden?
	Wo liegt derzeit die Höchststrafe bei einer Geldstrafe?
	Welche arbeitsrechtlichen Konsequenzen können Arbeitnehmern drohen?
9	Welche Themen sind zur Wahrung des Datenschutzes noch wichtig?
	Was zählt zu den ergänzenden Fachschulungen?
	Wie oft sollte eine Datenschutzschulung wiederholt werden?
	Wozu dienen ergänzende Fachschulungen?
10	Was sind die 3 grundlegenden Sicherheitskriterien?

	Nennen Sie Beispiele für Schutzmaßnahmen für die Verfügbarkeit.
	Nennen Sie Beispiele für Schutzmaßnahmen für die Integrität.
	Nennen Sie Beispiele für Schutzmaßnahmen für die Vertraulichkeit.
11	Welche Vorkehrungen sollten Sie im Bezug auf Datenschutz treffen, wenn Sie Ihren Arbeitsplatz verlassen?
	Sie finden einen USB-Stick. Wie verhalten Sie sich?
	An wen wenden Sie sich bei Sicherheitsverstößen oder Fragen?
	Wie sind Passwörter zu dokumentieren?
12	Welche Methoden gibt es zur Authentifizierung?
	Sichere Passwörter sollten...
	Passwörter sollte man...
	Bei einem Verdacht auf Passwortklau, wie Verhalten Sie sich?
13	Wie sollten Sie sich am Arbeitsplatz verhalten?
	Was besagt die Clean-Desk-Policy?
	Welche Folgen kann eine Verletzung der Verhaltensregeln verursachen?
	Welcher Faktor ist in der Kette der Informationssicherheit am schwächsten?
14	Was darf der Arbeitgeber?
	Welche spezifischen Regelungen gelten bei der Personalbeschaffung?
	Was darf in der Personalbuchhaltung nicht gespeichert werden?
	Welche Vorgaben gelten in einer Sicherheitsabteilung?
15	Innerhalb welcher Zeit nach Kenntniserlangung, muss eine Datenpanne gemeldet werden?
	Nennen Sie Beispiele für meldepflichtige Vorfälle
	An wen wende ich mich bei Sicherheitsverstößen?
	Wozu wird eine Risikoanalyse bei einer Datenpanne durchgeführt?

Tabelle 4: Fragenkatalog

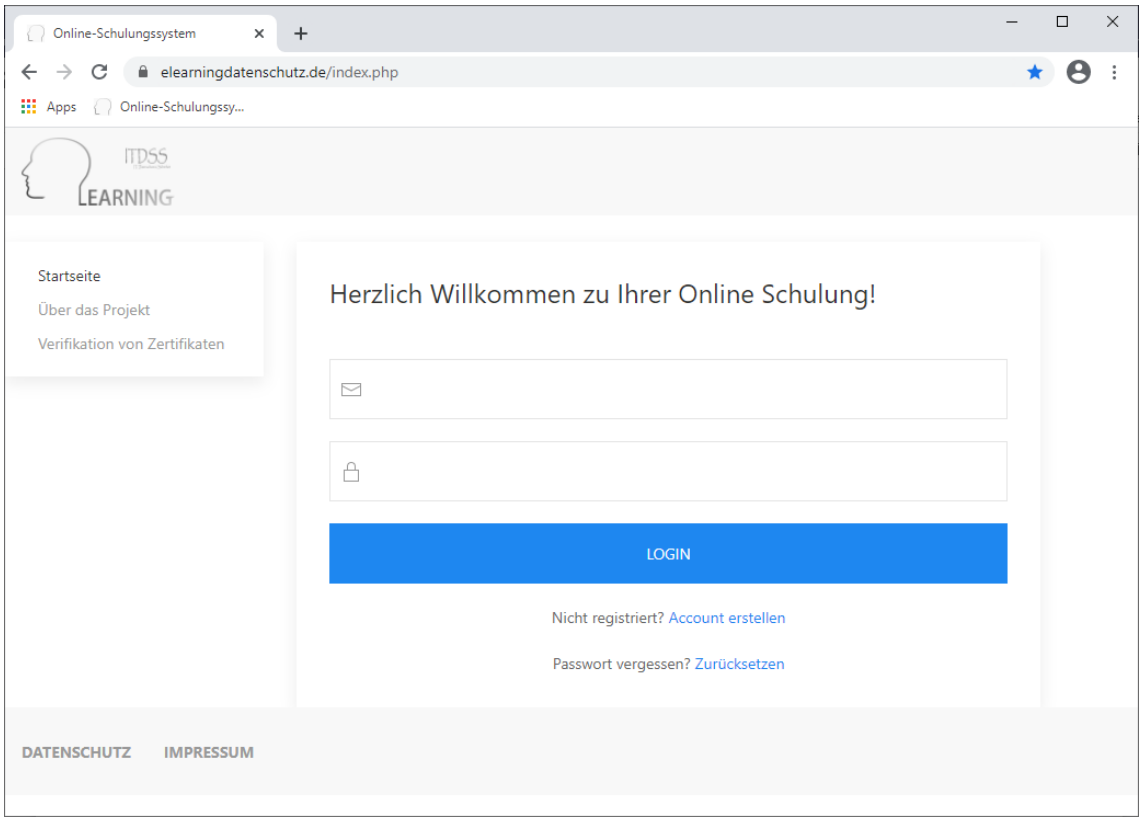

Abbildung 4: Startseite anonymer Bereich

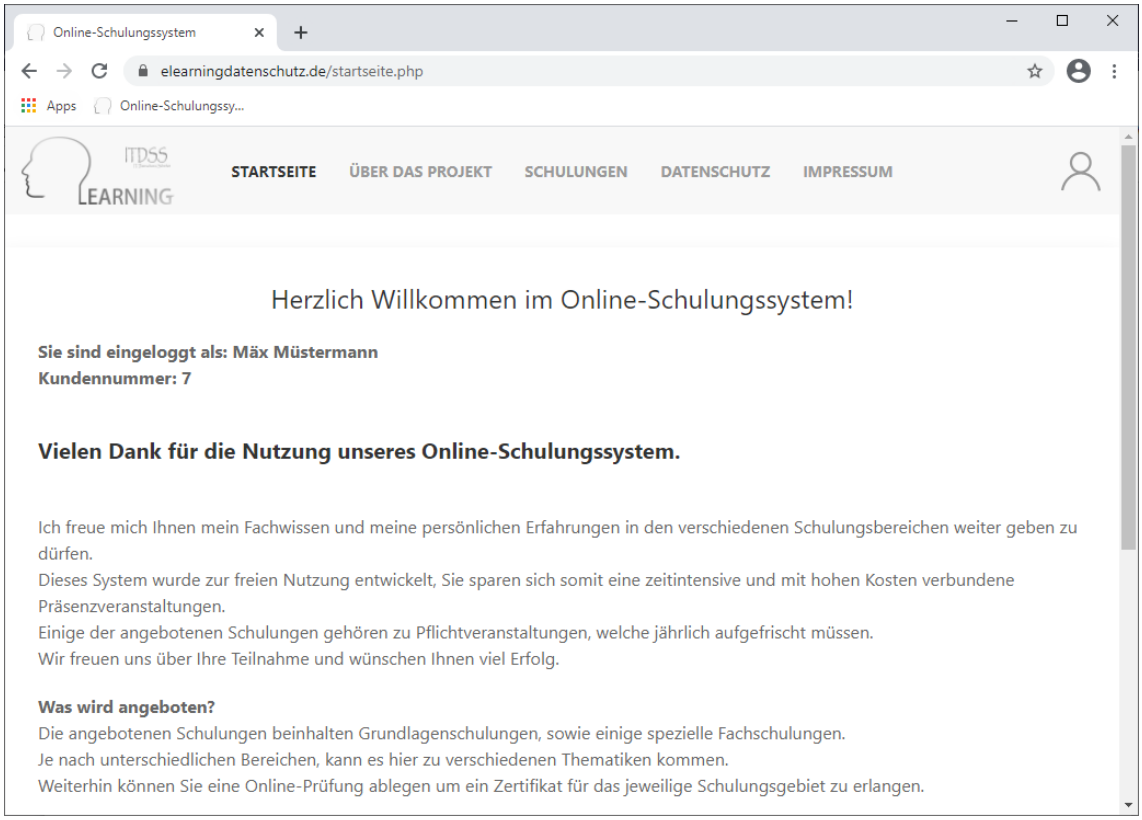

Abbildung 5: Startseite privater Bereich

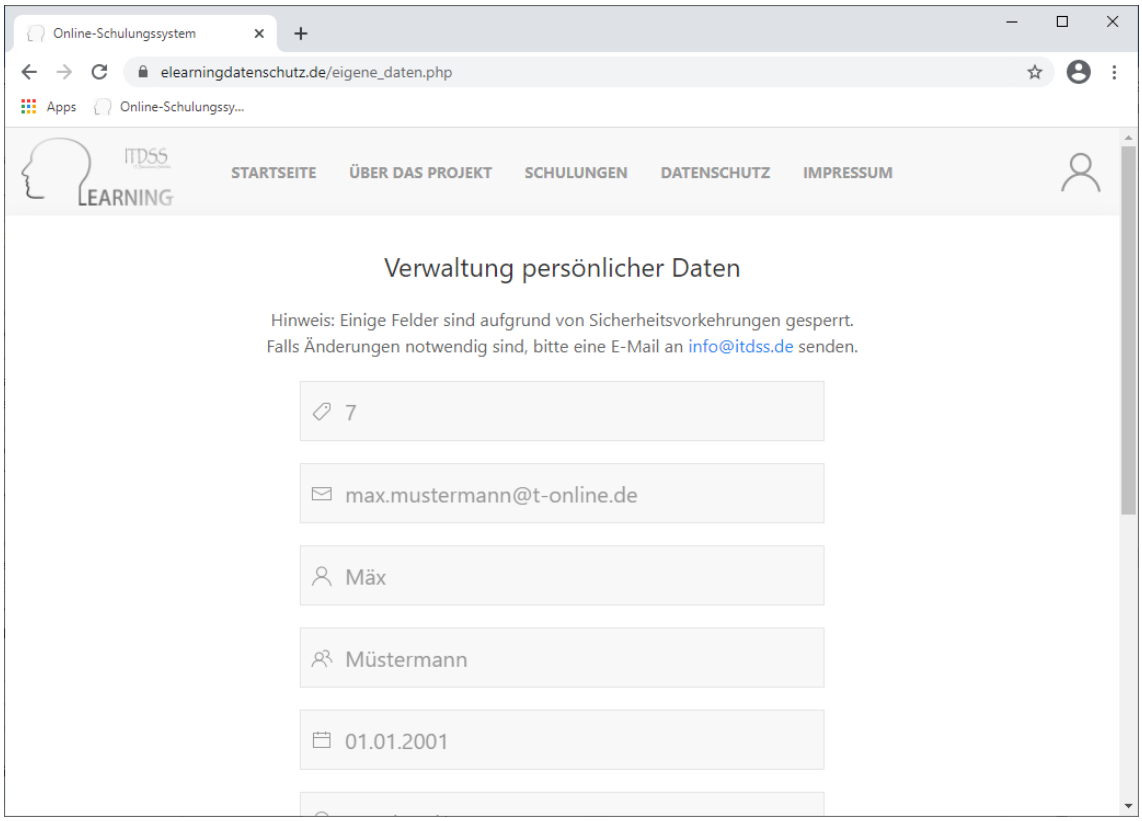

Abbildung 6: Verwaltung persönlicher Daten

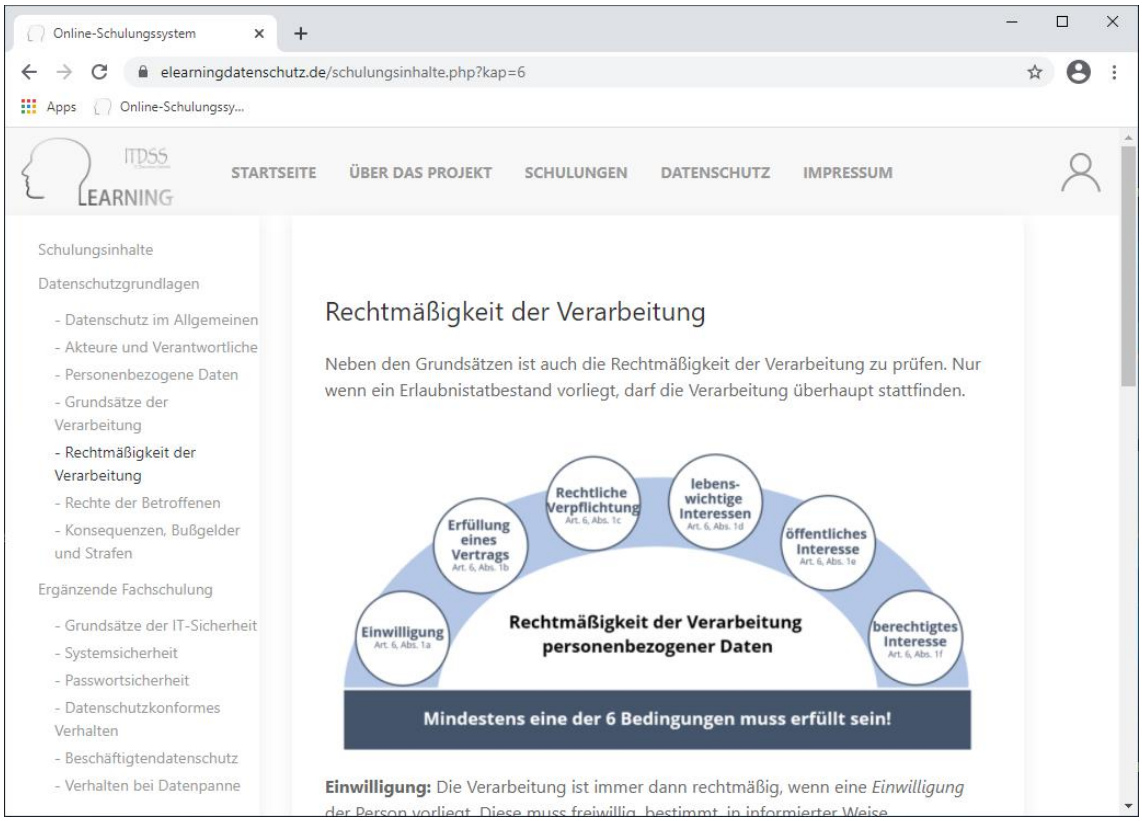

Abbildung 7: Datenschutzschulung

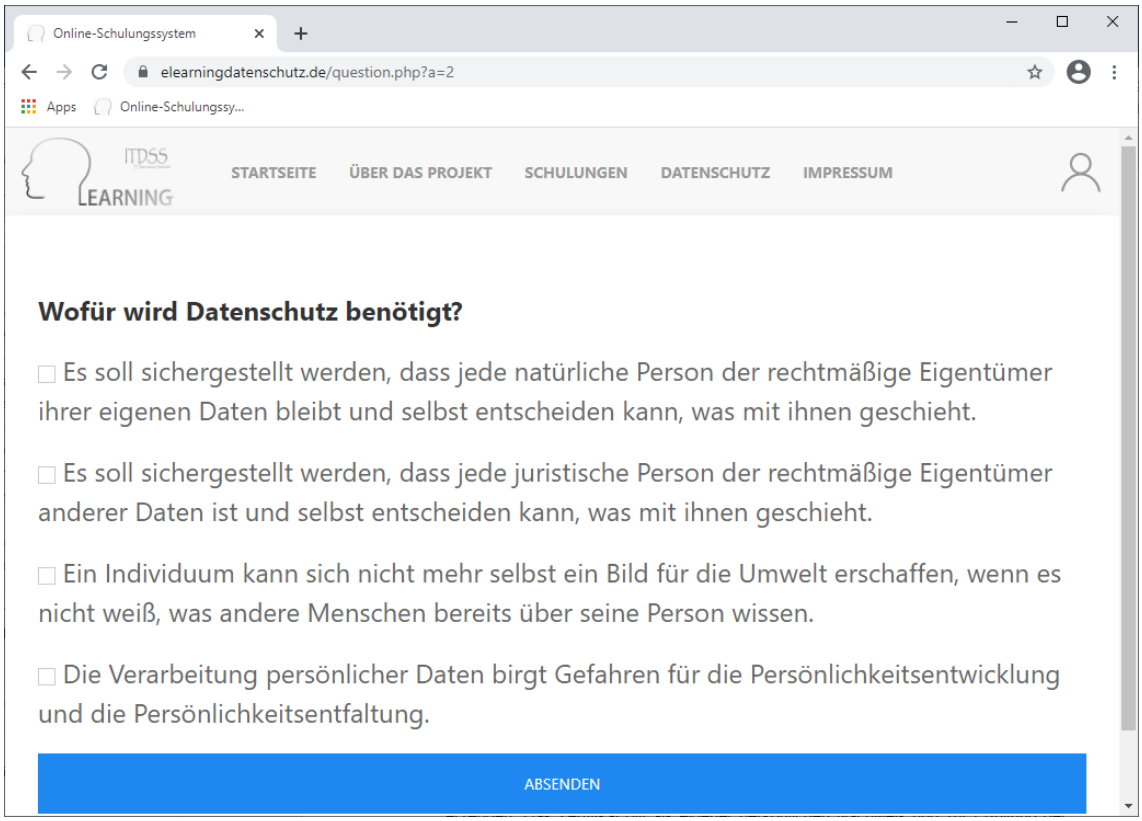

Abbildung 8: Prüfungen

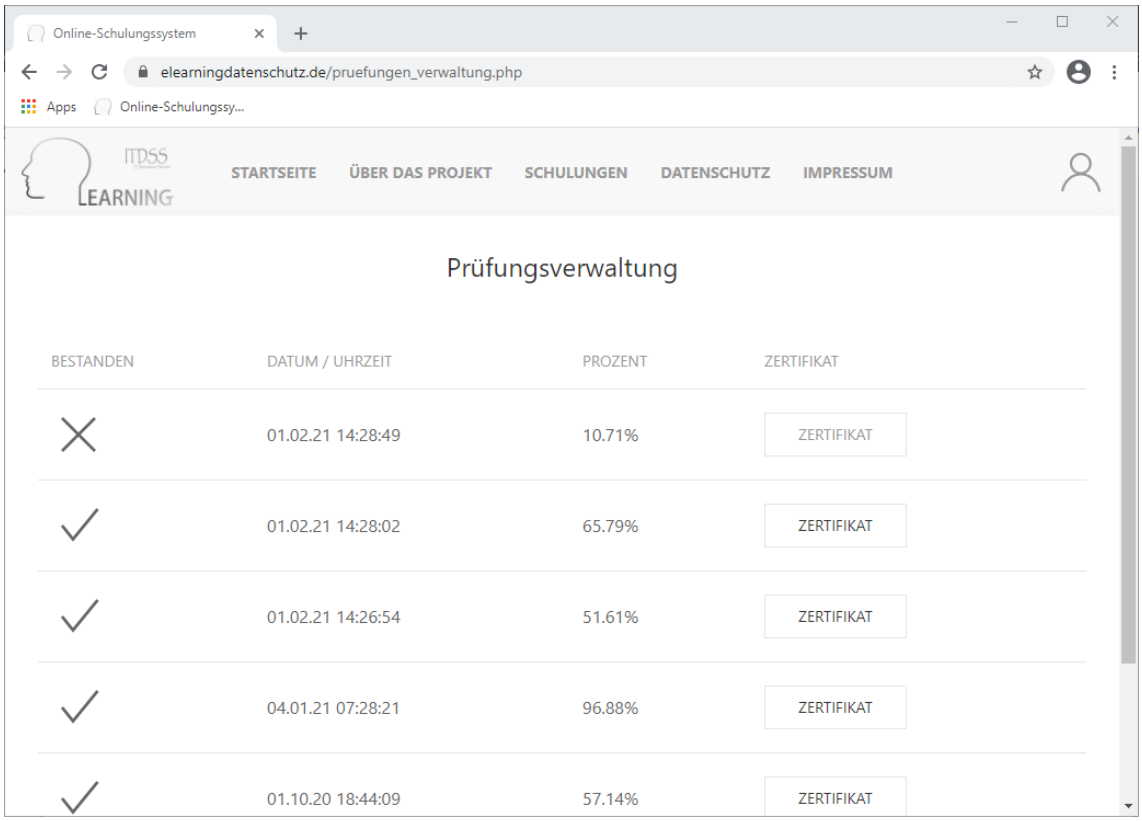

Abbildung 9: Prüfungsverwaltung

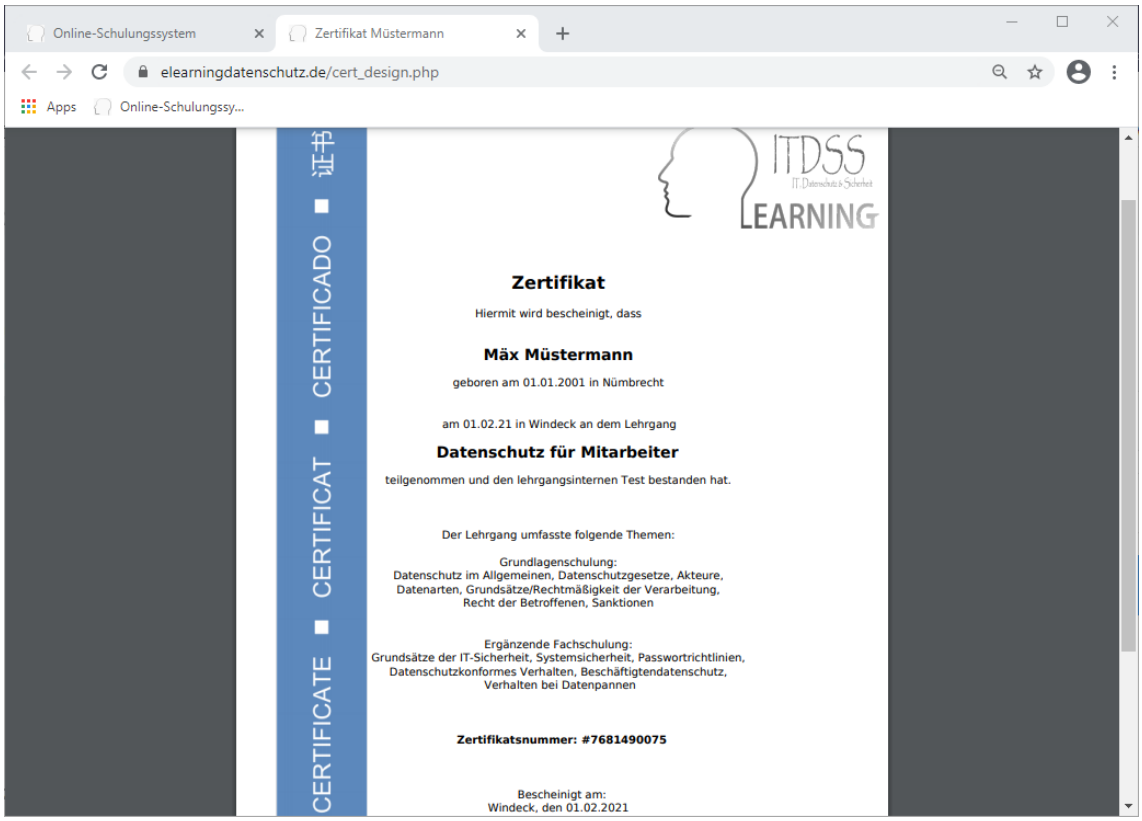

Abbildung 10: Zertifizierung

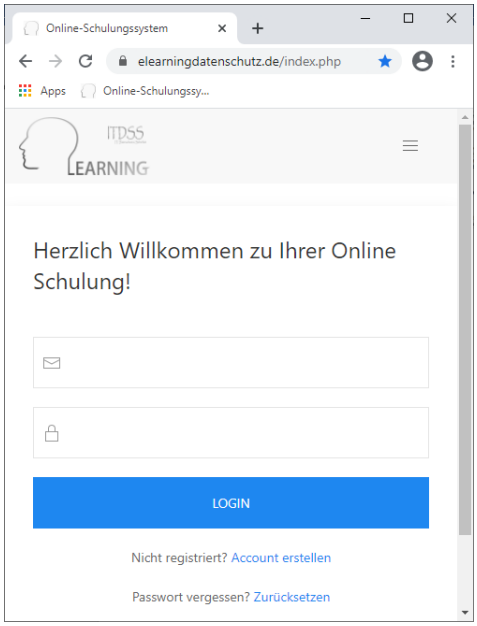

Abbildung 11: Responsive Design 1

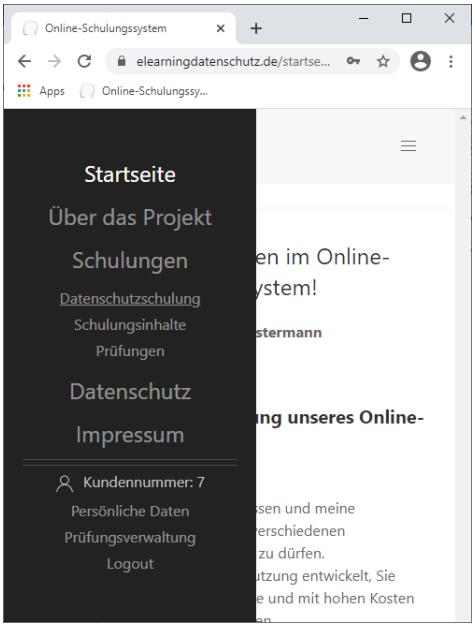

Abbildung 12: Responsive Design 2