Datenschutzfolgenabschätzung (DSFA) nach Artikel 35 EU-DSGVO

- Lernmanagementsystem itslearning -

Einführung:	10.08.2020
Ersteller:	III SVS L, beratend nach Art. 39 DSGVO DSB
Stand:	06.08.2020
Version	1.1

Gliederung

1. Einleitung und Vorgehen

Das Land Schleswig-Holstein plant, zum Beginn des neuen Schuljahres 2020/21, allen Schulen im Land das Lernmanagementsystem itslearning als zentral bereitgestellte Landeslösung im Sinne eines Angebots zur Verfügung zu stellen. Hierzu wurde im Rahmen der Produktauswahl und Vergabevorbereitung bereits eine datenschutzrechtliche Einschätzung vorgenommen und der Aufsichtsbehörde vorgestellt. Für die Sicherstellung der Datenschutzkonformität ist neben der Erstellung der notwendigen Dokumentation auch noch eine Datenschutzfolgenabschätzung nach Artikel 35 EU-Datenschutzgrundverordnung (DSGVO) durchzuführen.

Ziel dieser DSFA ist, auf Basis des risikobasierten Ansatzes des Standarddatenschutzmodells (SDM 2.0b) und den dort definierten Gewährleistungszielen die technischen und organisatorischen Maßnahmen zu bewerten und notwendige Anpassungen im Verfahren zu identifizieren, um die datenschutzrechtlichen Vorgaben zu erfüllen, die sich neben der DSGVO auch noch aus den Vorgaben von Schulgesetz (SchulG) und Schuldatenschutzverordnung (SchulDSVO) ergeben. Dabei sollen risikominimierende Maßnahmen, soweit wie möglich, bereits verfahrensseitig implementiert werden (privacy by design). Für die verbleibenden Restrisiken sollen organisatorischen Maßnahmen empfohlen werden, die dann auf Basis von Dienstanweisungen und Nutzungsordnungen verpflichtend vorgegeben werden.

2. Vorbereitende Maßnahmen

2.1. Schwellwertanalyse

Um die Notwendigkeit einer DSFA festzustellen, ist gemäß Artikel 35 DSGVO eine Vorabprüfung vorzunehmen und einzuschätzen, ob die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Kriterien für die Einschätzung ergeben sich aus dem Absatz 3 des Artikel 35, den durch die Artikel 29 Gruppe veröffentlichten Leitlinien[1] (WP248, Seite 10 ff.) und der nach Artikel 4 von der Aufsichtsbehörde veröffentlichten Liste von Verarbeitungsvorgängen[2], für die eine DSFA notwendig ist.

Eine DSFA ist aus Sicht der Artikel 29 Gruppe mindestens dann durchzuführen, wenn ein Verarbeitungsvorgang zwei oder mehr der in den obigen Quellen aufgeführten Kriterien erfüllt, da in diesem Fall von einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen ausgegangen werden kann.

[1] https://www.datenschutz-bayern.de/technik/orient/wp248.pdf
[2] https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf

Im Falle des betrachteten Verfahrens werden folgende Kriterien der Leitlinien (WP248) erfüllt und gehen grob mit den genannten Risiken einher (eine genauere Risikobetrachtung muss dann im Rahmen der DSFA erfolgen):

- Datenverarbeitung in großem Umfang (Nr. 5 der Liste in Anhang C)
    - Identitätsdiebstahl durch unbefugte Offenlegung von und Zugang zu Daten
    - Gesellschaftliche Nachteile bei Unrichtigkeit von Daten
    - Potenzielles Risiko durch die unklare Entwicklung zum EU-US-Privacy-Shield und dem Cloud-Act
    - ➔ Das Verfahren wird im Vollausbau ca. 400.000 Nutzende haben, die eigenständig Nutzdaten im großen Umfang erzeugen, welche zentral in Auftragsverarbeitung in einem kommerziellen Rechenzentrum (Amazon AWS – EU-Region) gespeichert werden.
- Daten zu schutzbedürftigen betroffenen Personen (Nr. 7)
    - Diskriminierung und Gefährdung durch unbefugte Offenlegung von und Zugang zu Daten
    - ➔ Daten von Schülerinnen und Schülern, die das System verpflichtend nutzen und sich der Verarbeitung auf Grund der Schulpflicht nicht entziehen können.
- Ansatzweise wird auch das Kriterium „Bewerten oder Einstufen“ erfüllt (Nr. 1)
    - Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte im Rahmen von Auswertefunktionen des Verfahrens
    - Gesellschaftliche Nachteile bei nicht zweckgebundener Verwendung

Somit ist gemäß Artikel 35 Absatz 1 DSGVO eine Datenschutzfolgenabschätzung durchzuführen.

2.2. Beschreibung der Verarbeitung

2.2.1. Kurzbeschreibung des Verfahrens und der Verarbeitungszwecke

Bei dem Produkt „itslearning“ handelt es sich um ein Lernmanagementsystem, welches vom Anbieter als SaaS (Software as a Service) angeboten wird. Der Betrieb in SH erfolgt als Landeslösung mit dem Ministerium für Bildung, Wissenschaft und Kultur (MBWK) als zentrale Stelle nach § 7 Abs. 4 Landesdatenschutzgesetz (LDSG). Hierdurch entfallen die sonst notwendigen individuellen Auftragsverarbeitungsverträge (AVV) zwischen Schule und Anbieter.

Mit diesem Lernmanagementsystem werden Funktionen zum Lernen auf Distanz, zur Kommunikation und Kollaboration, zum individualisiertem Lernen und zur Bereitstellung von Lernmaterialien in Abstimmung mit schulinternen Curricula und länderübergreifenden Fachanforderungen/Bildungsstandards, bereitgestellt. Ziel ist die Schaffung von

Möglichkeiten, digitale Medien und Werkzeuge für die Flexibilisierung von Unterricht zu nutzen und damit den Anforderungen an digitale Bildung gerecht zu werden.

Für die Nutzung des Systems werden zum Zwecke der Bereitstellung von Benutzerzugängen und die organisatorische Strukturierung der Funktionen (Schulebene, Klassenebene, Individualebene etc.) personenbezogene Daten verarbeitet (siehe 2.2.4.).

Bei der Nutzung werden durch die Benutzerinnen und Benutzer darüber hinaus individuelle Nutzdaten erzeugt und gespeichert, die ebenfalls personenbezogene Daten enthalten können (Konversationen, Rückmeldungen, persönliche Arbeitsergebnisse etc.). Zweck der Verarbeitung ist hier die Realisierung eines Online-unterstützten Lernens und der internen Kommunikation.

Nach der Grundeinrichtung des Systems auf Siteebene (alle Schulen in SH) erfolgt durch festgelegte Site-Administratorinnen und -administratoren die Einrichtung individueller Schulzugänge (teilnehmende Schulen).

Voraussetzung für die Teilnahme einer Schule ist die Erfüllung der notwendigen Voraussetzungen (Schulkonferenzbeschluss, örtliche Mitbestimmung, Festlegung von Verantwortlichkeiten, Erstellung der Verfahrensdokumentation aus zentral bereitgestellten Mustern).

Für die Generierung der schulspezifischen Benutzerkonten für die unterschiedlichen Gruppen von Nutzenden (Schuldministratorinnen und -administratoren, Lehrkräfte, Lernende, weiteres pädagogisches Personal, optional auch Eltern) wird eine Verknüpfung mit dem Schulportal-SH (Dataport), welches das Identitätsmanagement (Univention) beinhaltet, hergestellt. Über diese Schnittstelle werden die erforderlichen und zulässigen personenbezogenen Daten der Nutzenden schulscharf in itslearning eingepflegt und die Benutzerzugänge eingerichtet. Die Basisdaten werden für Schülerinnen und Schüler aus den (noch) unterschiedlichen Schulverwaltungsprogrammen exportiert und in das Schulportal eingelesen. Die Daten aller Lehrkräfte in SH werden, mit einer Dienststelleninformation versehen, aus KoPers exportiert und ebenfalls in das Schulportal eingelesen.

Innerhalb der jeweiligen Schule erfolgt dann in itslearning die Abbildung der Schulstruktur (Klassen, Kurse), die Zuordnung von Lehrkräften sowie Schülerinnen und Schülern auf Klassen und Kurse und ggf. eine Individualisierung des Systems hinsichtlich der verfügbaren Funktionen, Berechtigungen und des Erscheinungsbildes der Benutzeroberfläche.

Das so vorbereitete System kann nach Test und Freigabe sowie der entsprechenden Dokumentation in den Echtbetrieb überführt werden.

2.2.2. Betroffene Personen

Bei der Bereitstellung und Nutzung des Lernmanagementsystem werden Daten von Schülerinnen und Schülern, ggf. deren Eltern, Lehrkräften und weiteren mit der pädagogischen Arbeit an Schulen beschäftigte Personen (Lehrkräfte im Vorbereitungsdienst, Personen nach § 34 Abs. 6 SchulG) sowie im Rahmen von Projekten und Arbeitsgruppen auch externe Teilnehmerinnen und Teilnehmer (Gäste) und die genannten Personengruppen anderer Schulen.

2.2.3. Rechtsgrundlagen für die Verarbeitung

Die Verarbeitung der Benutzerkontendaten der Schülerinnen und Schüler erfolgt auf Basis des Artikel 6 Absatz 1 Buchst. e DSGVO in Verbindung mit § 30 Schulgesetz (SchulG) mit den in § 11 Absatz 4 der Schuldatenschutzverordnung (SchulDSVO) festgelegten Beschränkungen für pädagogische Systeme.

Sollten die Eltern oder externe Teilnehmerinnen und Teilnehmer ebenfalls Zugang zu itslearning erhalten, können die für den Schulbereich geltenden Rechtsvorschriften (SchulG, SchulDSVO) nicht angewendet werden. Daher ist hier eine Einwilligungslösung (Artikel 6 Abs. 1 Buchst. a Datenschutz-Grundverordnung DSGVO) notwendig.

Die Verarbeitung der Beschäftigtendaten für die Bereitstellung der Benutzerkonten erfolgt auf Basis des Artikel 88 DSGVO in Verbindung mit § 15 Landesdatenschutzgesetz und § 85 Landesbeamtengesetz.

2.2.4. Datenumfang der Verarbeitung

Für die Einrichtung eines Benutzerkontos sind mindestens Name, Vorname, Benutzername und Passwort erforderlich. Optional können im Benutzerprofil noch Adress- und Kontaktdaten, das Geburtsdatum und persönliche Angaben durch die Nutzenden ergänzt werden.

Im Rahmen der Nutzung fallen je nach Rolle unterschiedliche weitere Daten an, die auch personenbezogene Daten enthalten können. Es sind dies bei Personen in der Rolle

a) Lehrkraft
b) Schülerinnen und Schüler
c) Gäste
d) Eltern
e) Administratorinnen und Administratoren

2.2.5. Verarbeitungsprozesse

Die Verarbeitungsprozesse bestehen aus dem initialen Datenimport von Lehrkräften und Schülerinnen und Schülern, den administrativen Tätigkeiten während der Nutzung, dem Erstellen und Bearbeiten von Aufgaben im schulischen Kontext sowie auf den schulischen Kontext bezogene Kommunikation zwischen Lehrkräften und Schülerinnen und Schülern.

2.2.6. Technische Umsetzung / Auftragsverarbeitung

Das System wird als Software-as-a-Service vom Anbieter bereitgestellt. Mit dem Anbieter itslearning ist ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO geschlossen worden. Als Unterauftragsverarbeiter werden Amazon Webservices (AWS) für das Hosting und Cloudflare für den DDoS-Schutz eingesetzt. Das Hosting bei AWS findet ausschließlich in der EU-Region statt. Der Hauptserverstandort ist Frankfurt. Für Datensicherungszwecke werden ausschließlich Server im EU-Raum genutzt. Die Daten auf den Servern von AWS sind grundsätzlich verschlüsselt und zusätzlich verwaltet itslearning eigene Zertifikate zur Ver- und Entschlüsselung selbst (Customer provided Encryption Keys).

2.2.6.1. Anbieterseite

Das LMS itslearning nutzt das zentrale ID-Management des Schulportal-SH und eine Anmeldung erfolgt per SSO.

2.2.6.2. Nutzerseite

Auf Nutzerseite erfolgt der Zugriff von unterschiedlichen Endgerätetypen, die können schuleigene oder privat genutzte Endgeräte (Bring your own Device). Der Zugriff erfolgt primär über eine Webschnittstelle zusätzlich existiert, insbesondere für die Benachrichtigungsfunktion eine App. Die Kommunikation zwischen Endgerät und Dienst erfolgt transportverschlüsselt.

2.2.7. Übersicht der zu Grunde liegenden Dokumente

- Verzeichnis der Verarbeitungstätigkeiten schulseitig (VVT)
- Auftragsverarbeitungsvertrag zwischen MBWK und itslearning (AVV)
- IT-Konzept des Anbieters
- Zertifikate des Hostingdienstleisters AWS und dem Anbieter itslearning (ISO27001)
- Produkthandbücher unter https://help.itslearning.com/help/de-DE/ApplicationHelp.htm
- Rechte- und Rollenkonzept
- Speicher- und Löschkonzept
- Prüfbericht III DSB vom 05.06.2020

3. Durchführung der DSFA

3.1. Allgemeines zur Systematik der Gewährleistungsziele

Im Rahmen der Bewertung und der Risikoidentifikation des Lernmanagementsystems sind die Grundsätze für die Verarbeitung nach Artikel 5 DSGVO und die Artikel 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) sowie 32 (Sicherheit der Verarbeitung) zu beachten. Daraus abgeleitet formulieren sowohl das Standard-Datenschutzmodell (SDM) als auch, in Teilen, der BSI-Grundschutz, Gewährleistungsziele. Während der BSI-Grundschutz den Fokus auf die Datensicherheit legt, betrachtet das SDM die Einhaltung der Ziele und die vorhandenen Risiken aus Sicht der betroffenen Personen und deren Rechte und Freiheiten.

Folgende Gewährleistungsziele können von identifizierten Risiken betroffen sein bzw. sind einzuhalten, um den Vorgaben der DSGVO zum Schutz der Rechte und Freiheiten der betroffenen Personen zu genügen:

- Datenminimierung/Speicherbegrenzung
    - Bewertung der im automatisierten Verfahren verarbeiteten personenbezogenen Daten auf Erforderlichkeit hinsichtlich der verfolgten Zwecke
    - Bewertung der Maßnahmen zur Löschung personenbezogener Daten unter Beachtung des Art. 5 Abs. 1 Buchst e) DSGVO
- Transparenz
    - Vorhandensein und Vollständigkeit der vor Beginn der Verarbeitung bereitzustellenden Informationen nach Artikel 13
    - Vorhandensein und Vollständigkeit der Dokumentation zur Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2, insbesondere
        - Verzeichnis von Verarbeitungstätigkeiten
        - Beschreibung von Prozessen zur Wahrung der Betroffenenrechte
        - Rechte- und Rollenkonzept
        - Speicher- und Löschkonzept
- Intervenierbarkeit
    - Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12 Abs. 1 und Abs. 2 DS-GVO,
    - Identifizierung und Authentifizierung des Auskunftsersuchenden (Art. 12 Abs. 6 DSGVO),
    - Berichtigungsmöglichkeiten von Daten (Art. 16 DS-GVO),
    - Löschbarkeit von Daten (Art. 17 Abs. 1 DS-GVO),

    - Einschränkbarkeit der Verarbeitung von Daten (ehemals Sperrung, Art. 18 DS-GVO),
    - Datenübertragbarkeit (Art. 20 DS-GVO)

Zur Wahrung des Datenschutzes (Betroffenensicht) und der Datensicherheit (Technische Prozesse) sind die nachfolgenden Punkte zu bewerten. Hier können auch die Ergebnisse einer erweiterten Risikoanalyse nach BSI einfließen.

- Verfügbarkeit / Belastbarkeit
    - Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
- Integrität
    - Sicherstellung der Korrektheit (vollständig, unverändert) von Daten und der korrekten Funktionsweise von Systemen.
    - Schutz vor unerlaubter Veränderung, Verfälschung, Manipulation oder Löschung.
- Vertraulichkeit
    - Schutz vor unbefugter Preisgabe von Informationen
- Nichtverkettbarkeit
    - Getrennte Verarbeitung nach Zweck (Funktionstrennung)
    - Ggf. getrennte Speicherung nach Zweck (Datentrennung)

Ziel muss es sein, durch technische und organisatorische Maßnahmen zu einer wirksamen Risikominimierung zu gelangen.

3.2. Risikoidentifikation und -analyse (Angreifer, Motive, Ziele, Szenarien)

Szenarien:

1. Fehlerhafte Grundeinstellung des Lernmanagementsystems
   Betroffene Gewährleistungsziele:
    - Datenminimierung/Speicherbegrenzung (Funktionsumfang)
    - Vertraulichkeit (Sichtbarkeit von Daten, Zugriff durch Dritte)
    - Integrität
2. Fehlerhafter Benutzerimport Schulportal SH und Lernmanagementsystem
   Betroffene Gewährleistungsziele:
    - Integrität, Vertraulichkeit (Doppelte Nutzerkonten, Zugriffserlaubnis für nicht berechtigtes Personal)

3. Fehlerhafte Rechtevergabe bei der Benutzereinrichtung
   Betroffene Gewährleistungsziele:
   - Integrität (Veränderung fremder Daten durch erweiterte Rechte)
   - Vertraulichkeit (Zugriff auf fremde Konten und Daten)

4. Externer Angreifer, kompromittiertes Administratorenkonto
   Betroffene Gewährleistungsziele:
   - Integrität (Veränderung fremder Daten durch erweiterte Rechte)
   - Vertraulichkeit (Zugriff auf fremde Konten und Daten)

5. Interner Angreifer, kompromittiertes Nutzerkonto
   Betroffene Gewährleistungsziele:
   - Integrität (Veränderung fremder Daten durch erweiterte Rechte)
   - Vertraulichkeit (Zugriff auf fremde Konten und Daten)

6. Zugriff auf das System durch Zugang zu Endgeräten bei nicht erfolgter Abmeldung
   Betroffene Gewährleistungsziele:
   - Integrität (Veränderung fremder Daten durch erweiterte Rechte)
   - Vertraulichkeit (Zugriff auf fremde Konten und Daten)

7. Verlust privater Endgeräte
   Betroffene Gewährleistungsziele:
   - Integrität, Vertraulichkeit, sofern der Zugriff auf das LMS möglich ist

8. Lehrkräfte nutzen das Lernmanagementsystem, insbesondere die Bewertungsfunktionalität zur Erfassung von persönlichen Notizen oder Informationen, die nach Art und Umfang dem § 13 SchulDSVO (Digitale Klassenbücher) zuzuordnen sind.
   Betroffene Gewährleistungsziele:
   - Transparenz, Nichtverkettbarkeit (unzulässiger Nutzungsumfang außerhalb des definierten Zweckes und in Abweichung von den Datenschutzinformationen und dem VVT)
   - Vertraulichkeit (mögliche Offenlegung von Leistungsdaten und Verhaltensinformationen)
   - Datenminimierung (Überschreitung des zulässigen Datenumfangs)

9. Nutzende erfassen weitere personenbezogene Daten, die über den Umfang nach § 11 Abs. 4 SchulDSVO hinausgehen („Über mich“, Adresse, Telefon etc.)

Betroffene Gewährleistungsziele:

- Datenminimierung (unzulässiger Datenumfang in Abweichung von den Datenschutzinformationen und dem VVT)
- Vertraulichkeit (mögliche Offenlegung weiterer Kontaktdaten und unzulässige Nutzung)
- Nichtverkettbarkeit (Nutzung der zusätzlichen Daten zu Schulverwaltungszwecken außerhalb des Hauptzwecks)

10. Abfluss von Daten durch unzureichendes Datenschutzniveau von Unterauftragsverarbeitern („Cloud-Act“)
    Betroffene Gewährleistungsziele:
    - Vertraulichkeit (Zugriff durch Dritte, unzulässige Weiterverwendung)

11. Externer Angreifer, Hacking der itslearning Infrastruktur insbesondere Server
    - Vertraulichkeit (Zugriff durch Dritte, unzulässige Verwendung)
    - Verfügbarkeit (Datenverlust durch Löschung, Nicht-Erreichbarkeit des Verfahrens)
    - Integrität (Datenmanipulation)

3.3. Risikobewertung (Eingriffsintensität, Schutzbedarf, Eintrittswahrscheinlichkeit, Folgen)

Szenario (lfd. Nr. aus 3.2)	Bewertung (Eintrittswahrscheinlichkeit gering, normal, hoch und schwere des Schadens geringfügig, überschaubar, substanziell, groß)	Maßnahme zur Risikominimierung
1	Eintrittswahrscheinlichkeit: normal Schadenshöhe für die Betroffenen: geringfügig	Frühzeitige Einbindung DSB, Identifikation zu deaktivierender Funktionen, Test- und Freigabe
2	Eintrittswahrscheinlichkeit: gering Schadenshöhe: geringfügig	KoPers als Datenquelle für die Lehrkräfte-Datensätze, SuS-Datensätze werden nur von der Schule bei Versandt über die Landesnetz-E-Mail-Adresse akzeptiert.
3	Eintrittswahrscheinlichkeit: gering Schadenshöhe: substanziell	Standardisiertes Rechte- und Rollenkonzept, getrennter Import von SuS und LK, automatisierte Erzeugung von Benutzerkonten im LMS über den Konnektor erzeugt. Sensibilisierung der Schul-Admins hinsichtlich der manuellen Einrichtung weiterer Konten.
4	Eintrittswahrscheinlichkeit: gering Schadenshöhe: substanziell	Systemseitige Aktivierung und zwingende Nutzung 2FA für System- und Schuladministratoren, begrenzte Anzahl der Administratorenkonten, Sensibilisierung der Administratoren
5	Eintrittswahrscheinlichkeit: gering	Nutzungsordnung und

	Schadenshöhe: überschaubar	Dienstanweisung zur Geheimhaltung von Passworten, Vorgaben zur Passwortkomplexität, Erzwungene Passwortänderung bei Erstanmeldung
6	Eintrittswahrscheinlichkeit: gering Schadenshöhe: überschaubar	§ 14 SchulDSVO, Nutzungsordnung, Dienstanweisung
7	Eintrittswahrscheinlichkeit: gering Schadenshöhe: geringfügig	Keine Datenspeicherung auf dem Endgerät
8	Eintrittswahrscheinlichkeit: hoch Schadenshöhe: überschaubar, in Kombination mit 4 substanziell	Deaktivierung der 360°-Berichte, Nutzungsordnung und Dienstanweisung
9	Eintrittswahrscheinlichkeit: normal Schadenshöhe: geringfügig	Nutzungsordnung
10	Eintrittswahrscheinlichkeit: gering Schadenshöhe: substanziell	Verschlüsselung der Daten bei AWS mittels Customer-Encryption-Keys. Verpflichtung des Anbieters zur Datenverarbeitung im DSGVO-Raum
11	Eintrittswahrscheinlichkeit: gering Schadenshöhe: substanziell	Zertifiziertes Rechenzentrum zusätzlicher DDoS-Schutz

4. Bewertung des Restrisikos hinsichtlich der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung

Im Vorwege der Erstellung der DSFA wurden bereits auf Basis des ersten Prüfberichts von III DSB kritische Punkte mit dem Anbieter besprochen und Anpassungen am System vorgenommen. Die Erkenntnisse sind in diese DSFA eingeflossen siehe 2.2.7.

Die erkannten Risiken können mit den ergriffenen Maßnahmen zur Risikominimierung auf ein akzeptables Restrisiko reduziert werden.

5. Test und Freigabe des Verfahrens (Nachweis der Risikominimierung)

Die Konfiguration des Verfahrens wurde geprüft und die Funktionen zur Gewährleistung der kritischen Arbeitsabläufe und Zugriffe wurden erfolgreich getestet und dokumentiert, siehe Test- und Freigabeprotokoll. Die identifizierten Maßnahmen zur Risikominimierung wurden umgesetzt. Da der Test erfolgreich verlaufen ist, kann das Verfahren freigegeben werden.