KONZEPT ZUR EINFÜHRUNG EINES DATENSCHUTZ- UND INFORMATIONSMANAGEMENTSYSTEMS IN DER ÖFFENTLICHEN VERWALTUNG

Antje Dietrich / Ina Klingele

Dr. Antje Dietrich, Professorin, Informationssicherheitsbeauftragte, Hochschule für öffentliche Verwaltung Kehl, Fakultät 2, Kinzigallee 1, 77694 Kehl, DE
dietrich@hs-kehl.de; http://www.hs-kehl.de

Dr. Ina Klingele, Professorin, Datenschutzbeauftragte, Hochschule für öffentliche Verwaltung Kehl, Fakultät 1, Kinzigallee 1, 77694 Kehl, DE
klingele@hs-kehl.de; http://www.hs-kehl.de

Schlagworte: ***Datenschutz, Informationssicherheit, Konzept für die öffentliche Verwaltung***

Abstract: *Gerade in aktuellen Krisenzeiten ist es umso wichtiger für die öffentliche Verwaltung und Hochschulen gegen Cyberangriffe geschützt zu sein. Daher stellen wir im folgenden Beitrag ein Konzept für die Einführung eines Datenschutz- und Informationssicherheitsmanagementsystems (DSMS/ISMS) vor, das an der Hochschule Kehl in Zusammenarbeit mit mehreren Gruppen von Studierenden, der Datenschutzbeauftragten und der Informationssicherheitsbeauftragten erarbeitet worden ist. Das Konzept wurde bereits an der eigenen Hochschule erfolgreich erprobt, so dass nun geeignete weitere Hochschulen oder auch Kommunen gewonnen werden sollen, um das Konzept dort ebenfalls anzuwenden und entsprechend ein passgenaues DSMS/ISMS einzuführen. Ein Baustein des Konzeptes ist die Aufnahme aller Prozesse in Form eines Verarbeitungsverzeichnisses und der Bewertung anhand Datenschutz- und Informationssicherheits-Kriterien. Darauf aufbauend werden die notwendigen Sollprozesse entwickelt, um den notwendigen Anforderungen zu entsprechen und um die Kriterien erfüllen zu können. Geeignete TOM (technische und organisatorische Maßnahmen) müssen getroffen werden, dafür werden zielgerichtete Vorschläge gegeben. Im Nachgang erfolgt eine regelmäßige Überprüfung.*

1. Zielsetzung

Nicht zuletzt durch den Krieg gegen die Ukraine hat sich die Sicherheitslage für öffentliche Einrichtungen verschärft. Verstärkt werden auch Hochschulen Opfer von gezielten Angriffen (Becker, Hochschulen im Visier). Die Verwaltungsvorschrift Informationssicherheit des Innenministeriums von Baden-Württemberg vom 07.04.2017 verpflichtet die Hochschulen des Landes, geeignete Managementsysteme einzuführen. Sobald es sich um die Verarbeitung personenbezogener Daten handelt, fordert die Datenschutz-Grundverordnung seit dem 25.05.2018 eine umfassende Rechenschaftspflicht der für die Datenverarbeitung Verantwortlichen ein. Das Standard-Datenschutzmodell der deutschen Datenschutzaufsichtsbehörden orientiert sich an den Bausteinen des IT-Grundschutz-Kompendiums des BSI (DSK, Das Standard-Datenschutzmodell Version 3.0, s. 65 f.; dazu a. Gollan, Datensicherheit, Rn. 1128; zur Identität zahlreicher Maßnahmen von Informationssicherheit und Datenschutz Rn. 1124). Die Anforderungen an ein systematisches Datenschutzmanagement und diejenigen an ein Informationssicherheitsmanagement sollten daher zur Aufwandsreduzierung in einem Konzept zusammengeführt werden (vgl. S. 3 Hochschulservicezentrum Baden-Württemberg; Umsetzungsvorschlag zu Datenschutz- & Informationssicherheitsmanagement, 2017). Daher wurde bereits 2018 das Pro-

jekt „Einführung eines Datenschutz- und Informationssicherheitsmanagementsystems (DSMS & ISMS)“ an der Hochschule Kehl als interdisziplinäres Lehrprojekt konzipiert (ausführlich Dietrich/Zitzmann, DSMS & ISMS, 2019). In Fortführung dieses Projektes wurden die personenbezogenen Daten verarbeitenden Prozesse an der Hochschule nunmehr erneut auf Schwachstellen aus Sicht des Datenschutzes und der Informationssicherheit überprüft und hieraus das Konzept für die Einführung eines Datenschutz-Informationsmanagementsystems (DSMS/ISMS) fortentwickelt.

1.1. Rechtliche Grundlagen DSMS an Hochschulen

Die 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; DS-GVO) fordert in Form von Dokumentations- und Rechenschaftspflichten ein systematisches Datenschutzmanagement. Diese europäische Verordnung ist in allen Mitgliedstaaten der EU unmittelbar geltendes Recht, lässt jedoch den einzelnen Mitgliedstaaten durch Öffnungsklauseln und Bereichsausnahmen insbesondere bei der Datenverarbeitung durch öffentliche Stellen zahlreiche Spielräume, die durch nationales Recht ausgefüllt werden (vgl. nur Martens, Datenschutzrecht, Rn. 899).

Der Anwendungsbereich der Datenschutz-Grundverordnung ist nur eröffnet, sobald personenbezogene Daten verarbeitet werden (Art. 2 Abs. 1 DS-GVO). Anonymisierte Daten unterfallen somit nicht dem strengen Regelungsregime der DS-GVO. Hierzu ist es notwendig, „dass der Personenbezug derart aufgehoben wird, dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann“ (Schild, in Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 4, Rn. 15a). Personenbeziehbare Daten unterfallen damit weiter dem Anwendungsbereich der DS-GVO, wobei bereits die Pseudonymisierung das Risiko für die Betroffenen senkt und personenbezogene Daten daher so schnell wie möglich pseudonymisiert werden sollen (vgl. Erwg. 26, 28 und 78 DS-GVO, zu den Anforderungen an eine datenschutzkonforme Pseudonymisierung vgl. Ernst in: Paal/Pauly, DS-GVO, Art. 4 DS-GVO, Rn. 41 ff.).

Mit der DS-GVO ist die Verarbeitung personenbeziehbarer Daten prinzipiell verboten, es sei denn, ein Erlaubnistatbestand liegt vor (vgl. Art. 6 DS-GVO). Gemäß Art. 6 Abs. 1 lit. e DS-GVO ist die Verarbeitung personenbezogener Daten rechtmäßig, sofern diese „für die Wahrnehmung einer Aufgabe erforderlich [ist], die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.“ Gemäß Art. 6 Abs. 1 lit. C DS-GVO ist eine Verarbeitung auch dann rechtmäßig, wenn sie „zur Erfüllung einer rechtlichen Verpflichtung erforderlich [ist], der der Verantwortliche unterliegt.“

Damit stellen Art. 6 Abs. 1 lit. c und lit. e DS-GVO für die öffentlichen Stellen die zentralen Erlaubnistatbestände zur Verarbeitung personenbezogener Daten dar, die jedoch gem. Art. 6 Abs. 3 DS-GVO durch unionsrechtliche oder nationale Erlaubnisnormen zu ergänzen sind (vgl. nur Martens, Datenschutzrecht, Rn. 899). Erlaubnisnormen für die baden-württembergischen Hochschulen finden sich insbesondere in § 12 Landeshochschulgesetz (LHG) und der gemäß § 12 Abs. 3 LHG zu erlassenden Datenschutzsatzung der einzelnen Hochschule. Im Übrigen gelten § 50 des Beamtenstatusgesetzes, die §§ 83–88 des Landesbeamtengesetzes und das Landesdatenschutzgesetz.

Wer personenbezogene Daten verarbeitet, unterliegt einer umfassenden Rechenschaftspflicht, Art. 5 Abs. 2, Art. 99 Abs. 2 DS-GVO. Alle Verarbeitungstätigkeiten, die der Zuständigkeit eines Verantwortlichen unterliegen, sind in einem Verzeichnis (Verzeichnis von Verarbeitungstätigkeiten) gemäß Art. 30 DS-GVO zu dokumentieren. Zudem verpflichtet Art. 32 DS-GVO die Verantwortlichen „geeignete technische und organisatorische Maßnahmen“ zu treffen, um „ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Hierzu zählt die DS-GVO neben „Pseudonymisierung und Verschlüsselung“ (lit. a) „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der

Verarbeitung auf Dauer sicherzustellen“ (lit. b), „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“ (lit. c) und „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen [TOM] zur Gewährleistung der Sicherheit der Verarbeitung“ (lit.d).

1.2. Rechtliche Grundlagen ISMS an Hochschulen

Die VwV Informationssicherheit des Innenministeriums Baden-Württemberg vom 7. April 2017 – 5-0275.0/ 25 – fordert die Einführung eines Managementsystems für Informationssicherheit bis zum 08.03.2018. Die Verordnung legt die Ziele, Grundsätze, Organisationsstrukturen und Maßnahmen für die Etablierung eines ganzheitlichen Informationssicherheitsprozesses fest. Auch für die Hochschule Kehl ist die VwV Informationssicherheit anwendbar, da es sich nach dem LHG um eine Einrichtung der Landesverwaltung Baden-Württemberg handelt.

Vorgaben der VwV Informationssicherheit (Informationssicherheitsleitlinie gemäß IT-Grundschutz) sind die folgenden Sicherheitsgrundsätze:

– Alle Dienststellen und Einrichtungen der Landesverwaltung setzen die Informationssicherheit gemäß IT-Grundschutz (BSI Standards 100-1 bis 100-3) um.
– Für die Landesverwaltung Baden-Württemberg wird ein Informationssicherheitsmanagementsystem (ISMS) in Anlehnung an die internationalen Standards (ISO = International Standardization Organization) unter Berücksichtigung des nationalen BSI Standards 100-1 »Managementsysteme für Informationssicherheit« eingeführt (ISO 27001 in der Ausprägung BSI IT-Grundschutz). Dieses ISMS umfasst Ressourcen, Prozesse und Konzepte für die Informationssicherheit in der Landesverwaltung Baden-Württemberg. Das ISMS legt fest, mit welchen Regelungen und Methoden die Aufgaben und Aktivitäten in Bezug auf die Informationssicherheit initiiert, gesteuert und überwacht werden.

2. Konzept für die Einführung eines Datenschutz- und Informationssicherheitsmanagementsystems (DSMS/ISMS)

2.1. Datenschutz-Managementsystem (DSMS)

Die genauen Anforderungen an ein Datenschutz-Management System sind umstritten (Scheja/Reibach/Reichert, in: Leupold u.a., IT-Recht, Teil 6.6 Rn. 4). Die deutschen Aufsichtsbehörden haben mit dem Standard-Datenschutzmodell eine Methode zur Datenschutzberatung und -Prüfung auf der Basis einheitlicher Gewährleistungsziele entwickelt, die aktuell in der Version 3.0 am 24.11.2022 durch die 104. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder beschlossen wurde. Im Vordergrund steht dabei die Rechenschafts- und Nachweispflichten als dauerhafte Aufgabe und somit als zyklischen Prozess mit dem aus dem Qualitätsmanagement bekannt und bewährten PDCA-Zyklus (Plan, Do, Check, Act) zu etablieren (DSK, Das Standard-Datenschutzmodell Version 3.0, S. 56). Die einzelnen Verarbeitungstätigkeiten sind somit nicht nur unter Angabe der Rechtsgrundlage und der TOM in einem Verarbeitungsverzeichnisses gemäß Art. 30 Abs. 1 DS-GVO zu erfassen, sondern auf Basis der einheitlichen Gewährleistungsziele zyklisch zu überprüfen, ergänzt um eine bis zur Datenschutz-Folgenabschätzung führende Risikobewertung (vgl. auch Scheja/Reibach/Reichert, in: Leupold u.a., IT-Recht, Teil 6.6 Rn. 50 ff.).

2.2. Informationssicherheitsmanagementsystem (ISMS)

Grundsätzlich sollte nach einem systematischen Ansatz der Standard für Informationssicherheit innerhalb einer Organisation gesetzt werden. Wesentlich sind dabei das Engagement des Managements, die klare Einhaltung der Richtlinien und Verfahren / Prozesse, die Bewertung von Risiken, die Ableitung und Umsetzung von Maßnahmen zur Risikosenkung, die angemessene Kontrolle / Überwachung der Wirksamkeit, die Awareness (Schulungen, Informationen, Hilfestellungen) und die ständige Verbesserung (KVP) und Lernfähigkeit. Zentrale Themen der Informationssicherheit bzw. der physischen Sicherheit sind beispielsweise Zugang und Passwörter, E-Mail-Nutzung, Internetnutzung, Anti-Virus, Mobile Devices, Wechseldatenträger, Löschen von Informationen und die Behandlung von Sicherheitsvorfällen.

2.3. Datenschutz- und Informationssicherheitsmanagement (DSMS/ISMS)-Konzept an der Hochschule Kehl

2018 wurde mit der Einführung eines Datenschutz- und Informationssicherheitsmanagementsystems an der Hochschule für öffentliche Verwaltung in Kehl begonnen (Dietrich/Zitzmann, DSMS & ISMS, 2019). Das Kernprojektteam wurde hierzu durch drei Gruppen von Studierenden (in Summe 67 Studierende) aus den Vertiefungsbereichen Personal und Organisation und der IT-Vertiefung des Bachelor-Studienganges „Gehobener Verwaltungsdienst – Public Management“ im Wintersemester 2018/19 unterstützt, die zum einen im Bereich Datenschutz die verschiedenen Verfahren der Hochschule erfassten und bewerteten sowie zum anderen die für eine Hochschule relevanten Themen im Bereich Informationssicherheit bestimmten und ausarbeiteten. Seitdem wird das Konzept durch das Kernprojektteam fortgebildet.

Im Wintersemester 2022/2023 wurde nunmehr mithilfe zweier Studierenden- Gruppen aus der Vertiefung Personal, Organisation und Kommunikation und einer Gruppe der IT-Vertiefung (in Summe knapp 70 Studierende) eine umfassende Überprüfung der bestehenden Prozesse und Maßnahmen durchgeführt, um kontinuierlich die Hochschule in den Themenfeldern Informationssicherheit und Datenschutz weiter entwickeln zu können.

2.3.1. Projektbeschreibung

- *Projekttitel:* Einführung Datenschutz- und Informationssicherheitsmanagement
- *Projektziel:* Grundlagen schaffen für die Einhaltung der rechtlichen Vorgaben gem. DSG-VO und nationalem Recht sowie der VwV Informationssicherheit.
- *Zu erarbeitende Ergebnisse:* Erarbeitung eines Datenschutz- (DSMS) & Informationssicherheitsmanagementsystems (ISMS)
- *Meilensteine / zentrale Arbeitspakete:*

  Datenschutz / IT-Sicherheit:
  - Leitlinie bis Ende 10/2018
  - Bestandsaufnahme bis Ende 11/2018
  - Identifizierung des Handlungsbedarfs bis Ende 2/2019
    - Ermittlung Soll-Zustand
    - Lückenanalyse Ist-Soll
  - kontinuierliche Anpassung und Überprüfung
- *(Kern-)Projektteam:* Datenschutzbeauftragte; Informationssicherheitsbeauftragte; Leiter Hochschul-Rechenzentrum; Kanzler als Schnittstelle zum Rektorat; CISO; für die Umsetzung des Datenschutzes zuständige Koordinatorin. Im Laufe der Zeit kam es zu personellen Wechseln, insbesondere in der Position

der Datenschutzbeauftragten, seit 2021 konnte die Position des Chief Information Security Officer an der Hochschule besetzt werden, der das (Kern) Projektteam komplettiert.

- *Kommunikationsroutine:*
  - Etablierung eines vierzehntägigen Jour fixe des (Kern-)Projektteams
  - Newsletter an alle Mitarbeitenden und Studierenden zu den Themen Datenschutz und Informationssicherheit
  - Regelmäßige Berichte gegenüber dem Rektorat der Hochschule
  - Ergänzung der Rektoratsvorlagen um die standardmäßige Abfrage der relevanten Einbeziehung von DSB und ISB

2.3.2. Das Datenschutz-Managementsystem an der Hochschule Kehl

Das Datenschutz-Managementsystem setzt sich aus folgenden Bausteinen zusammen:

1. Rechtliche Grundlagen, insbesondere Satzung der Hochschule für öffentliche Verwaltung Kehl über die Verpflichtung zur Angabe von personenbezogenen Daten sowie über die Verarbeitung von personenbezogenen Daten zur Erfüllung der Aufgaben der Hochschule (Datenschutzsatzung) vom 18.02.2022 und Rechenschaftspflicht
2. Leitlinie Datenschutz und Informationssicherheit vom 27.03.2019
3. Klärung von Organisation, Rollen und Verantwortlichkeiten
4. Dokumentation: Ablage / erweitertes Verzeichnis der Verarbeitungstätigkeiten; Richtlinien
5. Home Office Empfehlungen
6. Datenschutz-Management: technische und organisatorische Maßnahmen (TOM); Einwilligungsmanagement
7. Datenschutz bei der Auftragsvergabe, Auftragsdatenverarbeitungsverträge, Vereinbarungen bei gemeinsam Verantwortlichen
8. Prozess zur Wahrnehmung der Betroffenenrechte (Informationspflichten, Anfragenmanagement)
9. Meldepflichten und Prozess Datenpanne
10. kontinuierliche Überwachung
11. Schulung & Sensibilisierung, Clean Desk Policy

In Baden-Württemberg wurde durch den Gesetzgeber die Ausfüllung der Rechtsgrundlage, die zuvor in der Hochschul-Datenschutzverordnung (HDSVO) geregelt war, in die Autonomie der Hochschulen gegeben (§ 12 Abs. 3 LHG), so dass nunmehr jede Hochschule die Einzelheiten der Verarbeitung personenbezogener Daten zur Erfüllung der Aufgaben der Hochschule mittels Satzung regelt.

Spezifisch datenschutzrechtlich wurde bei ausgewählten Prozessen das Einwilligungsmanagement überprüft, zumal Behörden aufgrund des vorhandenen Ungleichgewichts im Regelfall die Einwilligung nicht als gültige Rechtsgrundlage heranziehen können (vgl. Erwgr. 43 S. 1 DS-GVO).

In Baden-Württemberg besteht eine Anbietungspflicht aller Unterlagen, die zur Erfüllung der Aufgaben nicht mehr benötigt werden, an das Landesarchiv bzw. an eigene Archive (§§ 3 Abs. 1, 8 Landesarchivgesetz). Löschkonzepte müssen dieses daher berücksichtigen.

Insbesondere bei den Themen Home Office Empfehlungen, technische und organisatorische Maßnahmen, IT-Sicherheitsvorfall als Datenpanne, Schulung und Sensibilisierung, Clean Desk Policy bot sich eine gemeinsame Verfahrensweise im Rahmen des Informationssicherheitsmanagements an, die im Folgenden vorgestellt wird.

2.3.3. Informationssicherheitsmanagement an der Hochschule Kehl

Im Themenbereich Informationssicherheit wurden die technischen und organisatorischen Maßnahmen bezogen auf einen sicheren Arbeitsplatz an der Hochschule sowie im Home Office von einer Gruppe von Studierenden weiterentwickelt. Es wurde eine Handlungsempfehlunge erstellt, sodass Mitarbeitende der Hochschule Kenntnis darüber erlangen, wie Passwörter zu vergeben sind, welche Speichergeräte genutzt werden dürfen, wie sich bei der Internetnutzung und wie bei der Kommunikation zu verhalten ist. Dabei wurde auf die verschiedensten Endgeräte und auch auf „Bring your own Device“ eingegangen.

Eine weitere Gruppe beschäftigte sich mit den Melde- und Benachrichtigungspflichten bei Datenpannen und Sicherheitsvorfällen. Der aktuelle Meldeprozess der Hochschule wurde geprüft und entsprechend der Erkenntnisse der Studierendengruppe überarbeitet und angepasst. Es wurde ein Aushang entwickelt, der nun in jedem Raum der Hochschule ausgehängt werden wird, um im Krisenfall bei einen Sicherheitsvorfall entsprechend schnell reagieren zu können.

Eine Gruppe beschäftigte sich mit dem Notenverwaltungs- und Notenbekanntgabe System der Hochschule, das als besonders sensibel anzusehen ist. Schwerpunktmäßig wurde die Anbindung an die neue Hochschul-App aus Sicht der Informationssicherheit und des Datenschutzes geprüft.

Ein weiterer großer Themenkomplex war die Planung digitaler Prüfungen an der Hochschule Kehl und die Bewertung aus Datenschutz und Informationssicherheit Sicht. Dabei prüften die Studierenden vier verschiedene gängige Arten der digitalen Prüfung: digitale Prüfung als Vor-Ort-Prüfungen, digitale Prüfung außerhalb der Hochschule, onlinebeaufsichtigte Prüfungen, digitale Open Book und Take Home Prüfungen. Auch die Verwendung digitaler Hilfsmittel und digitaler Gesetzessammlungen wurde umfassend bewertet.

Ebenso wurde das aktuelle Lernmanagementsystem Moodle der Hochschule aus Sicht des Datenschutzes und der Informationssicherheit prüft. Dabei wurde auf aktuell verwendete Plugins schwerpunktmäßig Bezug genommen.

Ein weiteres Thema war die Erstellung eines Konzeptes zur sicheren E-Mail-Kommunikation mit der Hochschule, da dies gerade im Bereich der Masterstudiengänge (Kommunikation mit Afrika und EU) eine Anforderung war.

Die Übersicht der Assets (Hardware Assets und Software Assets) wurde weiter gepflegt.

Außerdem flossen die Ergebnisse der Studierenden sowie die Arbeitsergebnisse von den hilfswissenschaftlichen Arbeitskräften und natürlich der DSB, der ISB und des CISOs mit ein. Auch die regelmäßigen Newsletter wurden mit den Ergebnissen angereichert. Zudem fand im aktuellen Sommer- und Wintersemester eine umfassende Sensibilisierungskampagne im Bereich der Informationssicherheit für die Mitarbeitenden der Verwaltung und die Professorenschaft statt.

Im Bereich der Informationssicherheit sind anstehende Aufgaben, den ersten Vorschlag für eine Risikomanagementsystem und ein Notfallkonzept im Sinne des Business Continuity Managements für die Hochschule weiterzuentwickeln und im ISMS aufzunehmen. Daraufhin muss eine Bewertung in Form einer Business-Impact-Analyse erfolgen, so dass in der Phase der kontinuierlichen Verbesserung die anstehende Sensibilisierungskampagne für die Mitarbeitenden und die Professorenschaft angepasst werden kann. Letztendlich muss in der Projektphase der Überwachung, aufbauend auf ersten Vorschlägen von Studierenden, ein Auditkonzept umgesetzt werden. Dafür sollten entsprechende Kennzahlen verwendet werden, die ebenfalls bereits von einer Gruppe Studierender erarbeitet worden sind. Diese sollen die Grundlage für regelmäßige Reviews sein, die zur Vorbereitung eines Audits dienen können.

2.4. Studierendenprojekt zur Überprüfung

Im Rahmen des Vertiefungsschwerpunktes Personal, Organisation und Kommunikation des Bachelorstudienganges „Gehobener Verwaltungsdienst – Public Management" wurde im Wintersemester 2022/23 neben der kontinuierlichen Fortschreibung des Konzeptes durch das Kernprojektteam und die Verwaltung eine umfassende Überprüfung der laufenden Prozesse eingeleitet. Basis waren dabei 44 von den Beauftragten für Datenschutz und Informationssicherheit ausgewählte Prozesse, die entweder neu eingeführt wurden und werden oder bei denen Verbesserungspotenzial erkannt wurde. Jeder Studierende war Teil eines Teams von 2–3 Studierenden, die die entsprechenden Themenstellungen im Verlauf eines Semesters abzuarbeiten hatten. Für die Studierenden wurde diese Mitarbeit als Prüfungsleistung anerkannt.

Als Teil des Projektes interviewten die Studierenden hierzu die innerorganisatorischen Ansprechpersonen für die einzelnen Verarbeitungstätigkeiten, modellierten die Prozesse mithilfe erweiterter ereignisgesteuerter Prozessketten (eEPK) und führten eine Risikobeurteilung sowie ggf. Schwachstellenanalyse durch. Die so entstandenen Empfehlungen und modellierten Soll-Prozesse wurden im Rahmen einer Präsentation den innerorganisatorischen Ansprechpersonen vorgestellt. Anschließend wurde dieses durch die Studierenden schriftlich ausgearbeitet. Hierbei war ggf. auch die Dokumentation im Verzeichnis für Verarbeitungstätigkeiten anzupassen, wobei auf die Vorlage der Zentralen Datenschutzstelle der baden-württembergischen Universitäten mitsamt Ausfüllhinweisen zurückgegriffen werden konnte (ZENDAS, Vorlage VVT).

3. Ausblick

Im Rahmen des Projektes konnten die Studierenden als zukünftige Mitarbeitende in der Verwaltung des Landes Baden-Württemberg für die Bereiche Datenschutz und Informationssicherheit sensibilisiert werden. Zudem gelang es durch die zahlreichen Interviews mit unterschiedlichsten Ansprechpersonen in der Verwaltung der Hochschule auch die Mitarbeitenden nochmals für das Thema zu sensibilisieren, Ideen für Verbesserungsvorschläge aus der Reihe der Beschäftigten aufzunehmen und für die Verbesserungsvorschläge zu motivieren. Der Mehrwert für die Studierenden bestand darin, Einblicke in die vielfältigen Verwaltungsprozesse an einer Hochschule zu gewinnen und einen direkten Impact hinsichtlich erarbeiteter Verbesserungsvorschläge zu erzielen.

Das Konzept, ein Datenschutz- und Informationssicherheitsmanagementsystem einzuführen bzw. die vorhandenen Prozesse strukturiert überprüfen zu können, kann nunmehr mit zukünftigen Studierendengruppen auch jenseits der eigenen Hochschule eingesetzt werden.

Im kommenden Wintersemester ist die Erstellung umfassender Schulungsunterlagen zur Sensibilisierung der Studierenden und Mitarbeitenden der Hochschule in Bezug auf Datenschutz und Informationssicherheit geplant. Dazu sollen zur Unterstützung vor allem kurze Videoclips erstellt werden. Diese können auch von Kommunen zur Sensibilisierung der eigenen Mitarbeitenden verwendet werden. Somit kann auch zukünftig das erarbeitete Wissen der Studierenden nach außen und innen weitergegeben und multipliziert werden.

4. Literatur

Becker, Lilia, Hochschulen im Visier von Cyberkriminalität – Warum Lehr- und Forschungsinstitutionen zu Zielen werden, 18.05.2022, https://hochschulforumdigitalisierung.de/de/blog/hochschulen-im-visier-von-cyberkriminalitaet.

Dietrich, Antje / Zitzmann, Luis, Einführung eines Datenschutz- und Informationssicherheitsmanagementsystems, IRIS 2019

DSK (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder), Das Standard-Datenschutzmodell, Version 3.0., beschlossen am 24.11.2022, https://www.datenschutzkonferenz-online.de/media/ah/20221129SDM_Methode_V30.pdf

Gollan, Lutz, Technischer Datenschutz: Datensicherheit, in: Datenschutz in der Kommunalverwaltung, Hrsg. von Zielkerns, Martin/Gollan, Lutz, Erich Schmidt Verlag, 5. Aufl. 2019.

Hochschulservicezentrum Baden-Württemberg, Umsetzungsvorschlag zu Datenschutz- & Informationssicherheitsmanagement, Stand 08.07.2017.

Leupold, Andreas u.a., IT-Recht, Verlag C.H.Beck, 4. Aufl. 2021

Martens, Kay-Uwe, Datenschutzrecht, in: Schweickhardt/Vondung, Allgemeines Verwaltungsrecht, Hrsg. von Annette Zimmermann-Kreher, Verlag W. Kohlhammer, 11. Aufl. 2021.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz Grundverordnung, Verlag C.H.Beck, 3. Aufl. 2021.

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), BeckOK Datenschutzrecht, Verlag C.H.Beck, 42. Ed. Stand: 01.11.2022.

ZENDAS (Zentrale Datenschutzstelle der baden-württembergischen Universitäten), Vorlage Verzeichnis von Verarbeitungstätigkeiten, Besonderer Teil, 19.01.2018.