secjur

Die externen Dateninsider

Datenschutzkonzept
für
Samsung Neues Lernen

Stand: Dezember 2021

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Inhalt

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

1. Scope / Einleitung

Mit **Samsung Neues Lernen** ist die Samsung Electronics GmbH - im Folgenden „Samsung" genannt - in Kooperation mit qualifizierten Partnern wie der ANTARES PROJECT GmbH – im Folgenden „Antares" genannt –, die Betreiberin von Antares CS und Edu-Pool, Edu-Cap. Des Weiteren trägt die Classroom Management-App dem Lösungspaket für den Digitalpakt Schule bei, die im Auftrag von Samsung eigens für **Neues Lernen** durch die Tabnova, Inc. entwickelt wurde. Es werden Hard- und Software sowie Lern- und Lehrmaterialien für Schulen und Bildungsträger zu einem Gesamtkonzept gebündelt. Die Hardware für **Samsung Neues Lernen** besteht aus Android-Tablets für Schüler[1] und Lehrer, welche von der IT-Administration der Schule über eine Sicherheitslösung (Samsung Knox) verwaltet werden. Samsung Knox ist eine Kombination aus einer bewährten Sicherheitsbasis, und einer ausgereiften Suite von Geschäftslösungen, die diese Plattform nutzen. Die Knox-Sicherheitsplattform ist in die Geräte von Samsung integriert und sichert sie ab dem Zeitpunkt des Einschaltens mit mehrschichtigen Hardware- und Software-Sicherheitsfunktionen, welche immer aktiv sind. Die Knox-Plattform enthält übergreifende Abwehr- und Sicherheitsmechanismen, die die Daten vor Eindringlingen, Malware und anderen Bedrohungen schützen. Die Tablets werden mit einem Programm zur Klassensatz-Steuerung, der Samsung Classroom Management App und einer Lösung von Antares ausgestattet, mit welchen die Bereitstellung der von der Schule lizenzierten Lerninhalte organisiert werden können. So können Lehrer im Unterricht bestimmen, welche multimedialen Inhalte für die Schüler bereitstehen sollen. Mittels elektronischer Auswertungsbögen kann der Lernfortschritt überprüft werden.

Von Beginn an legte **Samsung Neues Lernen** großen Wert auf den Datenschutz aller beteiligten Schüler, Eltern und Lehrer. Die Konferenz der deutschen Aufsichtsbehörden im Datenschutz (DSK) hat eine Orientierungshilfe für den Einsatz von Online-Plattformen im Unterricht veröffentlicht, in welcher sie Vorgaben zum datenschutzkonformen Einsatz von Lernplattformen aufstellt.[2] **Samsung Neues Lernen** ist so entwickelt und

[1] Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern auf dieser Website die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

[2] https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

voreingestellt, dass sämtliche dieser Vorgaben eingehalten werden. Was dazu im Einzelnen nötig ist, ist Gegenstand dieses Datenschutzkonzepts.

Dieses Datenschutzkonzept hat damit zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte und Maßnahmen darzustellen, welche getroffen werden müssen, um die Regelungen zum Datenschutz bei der Implementierung der Lösungen von **Samsung Neues Lernen** einzuhalten. Hier wird beschrieben, wie sichergestellt werden kann, dass personenbezogene Daten im Einklang mit den regulatorischen Anforderungen verarbeitet werden. Es dient darüber hinaus auch als Grundlage für datenschutzrechtliche Prüfungen durch die verantwortliche Stelle oder deren Aufsicht, etwa den Schulträger der Einrichtungen, welche **Samsung Neues Lernen** einsetzen.

2. Die Akteure im Datenschutz

Das Datenschutzrecht dient dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und soll damit Grundfreiheiten sowie Grundrechte, insbesondere das Recht auf informationelle Selbstbestimmung, schützen. Seit dem Jahr 2016 gilt die von der Europäischen Union erlassene Datenschutzgrundverordnung (DSGVO). Damit soll das Datenschutzrecht in Europa weitgehend vereinheitlicht werden. Trotzdem gilt nicht in allen Mitgliedstaaten der Europäischen Union das gleiche Datenschutzrecht. Die DSGVO hat verschiedene sogenannte Öffnungsklauseln, die den Mitgliedstaaten Raum lassen, zu verschiedenen Datenverarbeitungsvorgängen eigene Regeln zu erlassen. Das betrifft besonders die Verarbeitung durch öffentliche Stellen und somit auch den schulischen Bereich. Beim Einsatz von **Samsung Neues Lernen** sind daher nicht nur die Vorgaben der DSGVO zu beachten, sondern ggf. auch die des Bundesdatenschutzgesetzes sowie die datenschutz- und schulrechtlichen Vorgaben der einzelnen Bundesländer. Für das bessere Verständnis werden zunächst die drei unterschiedlichen Rollen im Datenschutz erläutert, sowie der Begriff der personenbezogenen Daten näher erklärt.

2.1. Personenbezogene Daten und Betroffene

Dreh- und Angelpunkt des Datenschutzes ist das sogenannte personenbezogene Datum. Damit sind alle Informationen gemeint, welche sich auf eine identifizierbare oder identifizierte natürliche Person beziehen. Dies umfasst in einem denkbar weiten Verständnis alle Angaben, welche mit einer Person in Verbindung gebracht werden können. Dazu zählen neben Angaben,

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

wie z.B. Name, Klassenzugehörigkeit, Anschrift, etc. auch technische Merkmale wie etwa eine IP-Adresse (wenn die Möglichkeit besteht, deren Inhaber zu identifizieren).

Menschen, auf die sich personenbezogene Daten beziehen, heißen im Datenschutzrecht "Betroffene". Das sind beim Einsatz von **Samsung Neues Lernen** jeweils die Lehrenden und Lernenden.

2.2. Verantwortlicher

Um zu bestimmen, welche Organisation oder Behörde die jeweiligen Rechte und Pflichten aus dem Datenschutzrecht betreffen, muss zunächst festgestellt werden, welche die sog. verantwortliche Stelle bzw. der "Verantwortliche" im Sinne der DSGVO ist. Wichtigste Pflicht des Verantwortlichen ist es, jederzeit Rechenschaft über die Einhaltung aller datenschutzrechtlichen Pflichten ablegen zu können. Verantwortlicher ist jede juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Verantwortliche muss also nicht zwingend derjenige sein, der die Daten selbst erhebt oder verarbeitet. Er kann sich auch eines sogenannten Auftragsverarbeiters bedienen, welcher die personenbezogenen Daten für den Verantwortlichen verarbeitet. Der Verantwortliche im Sinne der DSGVO darf nicht verwechselt werden mit der zuständigen bzw. verantwortlichen Person innerhalb einer Organisation oder Behörde. Auch wenn innerhalb der Schule etwa die Schulleitung bei Entscheidungen über den Einsatz bestimmter Datenverarbeitungsvorgänge das letzte Wort haben mag, meinen wir in diesem Datenschutzkonzept im Gleichklang mit den Begrifflichkeiten des Datenschutzrechts die Schule bzw. den Schulträger daher als solche.

Wichtig ist, dass der Verantwortliche immer die Entscheidungshoheit über die Datenverarbeitung behält. Lehrende sollten im Rahmen ihrer Freiheit zur Gestaltung des Unterrichts digitale Lernplattformen wie etwa Antares CS und Edu-Pool daher nur in dem Umfang nutzen, wie dies von der Schulleitung (ggf. dem Schulträger) bzw. der Schulaufsicht festgelegt wurde. Die datenschutzrechtlichen Konsequenzen und Pflichten, die sich aus einem solchen Einsatz ergeben können, wären nämlich durch die Schule bzw. den Schulträger insgesamt zu erfüllen.

2.3. Auftragsverarbeiter

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Neben den Verantwortlichen gibt es im Datenschutzrecht sog. Auftragsverarbeiter. Dabei handelt es sich um Dienstleister, die bestimmte Datenverarbeitungen für einen Verantwortlichen durchführen. Wesentliches Merkmal einer Auftragsverarbeitung ist, dass der Auftragsverarbeiter nur auf konkrete Weisung des Verantwortlichen tätig wird. Inhalt und Umfang einer Auftragsverarbeitung müssen entsprechend der DSGVO in einem umfassenden Vertrag geregelt werden. Typisches Beispiel für eine Auftragsverarbeitung sind etwa Cloud-Services oder die Durchführung der Buchhaltung eines Unternehmens durch einen externen Anbieter. Im schulischen Bereich wären typische Beispiele etwa die Nutzung eines Webtools oder einer Videokonferenzsoftware.

3. Geplante Verarbeitungen

Es ist möglich, **Samsung Neues Lernen** mit einem Minimum an personenbezogenen Daten einzusetzen. So ist es etwa für Schüler nicht erforderlich, einen individualisierten Account z.B. bei Google oder Samsung anzulegen, um Tablets im Unterricht zu verwenden.

Die Kernkomponenten von **Samsung Neues Lernen** bestehen aus den Content-Schnittstellen-Apps EduCAP (Tablet), Antares- CS und EduPool (Web) zur Bereitstellung der digitalen Lerninhalte, der mobilen Sicherheitslösung Samsung Knox und dem Samsung Classroom Management. Mit allen Partnern, über deren Cloud-Infrastruktur der Betrieb von **Samsung Neues Lernen** ermöglicht wird, können Schulen bzw. deren Träger Verträge über eine Auftragsverarbeitung abschließen, sodass diese als die datenschutzrechtlich Verantwortliche Stelle die volle rechtliche Kontrolle behalten.

Für die Nutzung von **Samsung Neues Lernen** ist die Verarbeitung verschiedener personenbezogener Daten erforderlich. Details dazu sind im folgenden Abschnitt enthalte, wobei die Kategorisierung der personenbezogenen Daten der Orientierungshilfe der Datenschutzkonferenz folgt:

3.1. EduCAP

Mit der elektronischen Mediathek EduCAP (bzw. der Webvariante Edupool) lassen sich nicht nur freie Online-Inhalte offline nutzen, sondern es ist auch möglich, den Schülern einer Klasse individuelle Lerninhalte zuzuweisen und Apps zu installieren, für die das Land bzw. der Schulträger entsprechende Lizenzen erworben hat.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

- **Erforderliche Stammdaten** (Daten zur Anlage von Benutzerkonten sowohl für die Identifikation der Nutzer als auch zur Vergabe von Berechtigungen):
  Für die Nutzung von EduCAP verarbeitet Antares den Klarnamen, die Klassenstufe und den Namen der Schule. Diese werden genutzt, um eine sog. Edu-ID für jeden Lernenden anzulegen, die für das Einloggen in der Content-App EduCAP erforderlich ist. Bei der Edu-ID handelt es sich um ein Pseudonym. Sie dient damit dem Datenschutz durch Technikgestaltung[3].

- **Nutzungsdaten** (Daten, welche automatisch über Nutzer und deren Aktivitäten gespeichert werden):
  Die Nutzung und technische Kommunikation mit den Antares-Servern erfolgt ebenfalls über die Edu-ID.

- **Pädagogische Prozessdaten** (Informationen, welche dem Lehrer die Möglichkeit geben den individuellen und kollektiven Lernprozess nachzuvollziehen):
  Lehrer können sogenannte Auswertungsbögen (Lückentexte oder Multiple Choice Fragen) erstellen, um den individuellen Lernstand zu kontrollieren.

Die Edu-ID wird bis zum Ende eines Schuljahres benötigt und im Anschluss automatisch gelöscht.

3.2. Classroom Management-App

Mit der Classroom Management App behält die Lehrperson die Kontrolle über die Verwendung der Tablets im Unterricht und kann unter anderem Dateien verteilen, den eigenen Bildschirm auf den Schülertabletts anzeigen oder den Bildschirm der Schüler sperren.

Die Classroom Management App bietet je nach Einsatzzweck zwei unterschiedliche Modi. Die jeweiligen Datenflüsse und die erhobenen und verarbeiteten Datenkategorien unterscheiden sich je nach Anwendungsszenario. Zum einen kann die Classroom Management App im Präsensunterricht im Klassenraum eingesetzt werden, indem die Verbindung zwischen den Geräten über das WLAN der Schule hergestellt wird. Zum anderen kann Classroom Manage für

[3] Nach Art. 25 Abs. 1 DSGVO.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

den Fernunterricht eingesetzt werden. Die Verbindung der Endgeräte untereinander wird in diesem Fall über eine Cloud-Infrastruktur hergestellt.

(a) Präsenzunterricht

Für die Nutzung von Classroom Manage im Präsenzunterricht im Klassenraum werden die Daten wie folgt zwischen den an der Unterrichtseinheit beteiligten Endgeräten über das WLAN-Netzwerk der Schule ausgetauscht:

- **Erforderliche Stammdaten:**
  Name (für die Anzeige auf dem Lehrertablet bei der Anmelden an der Samsung Classroom Management-App, damit Lehrer die Unterrichtseinheit für Schüler aufsetzen und starten können)

- **Nutzungsdaten**:
  Die Schülertablets scannen einen QR-Code, der durch das Lehrertablet generiert wird. Dadurch treten Schüler dem vom Lehrertablet aufgesetzten Unterricht über das WLAN der Schule bei. Die technische Kommunikation geschieht dann ausschließlich über WLAN ohne Übermittlung von Nutzungsdaten an Dritte.

- **Pädagogische Prozessdaten**:
  Pädagogische Prozessdaten enthalten alle Dateien, welche während der laufenden Unterrichtsstunde erstellt werden. Über die Classroom Manage App lassen sich folgende Datenobjekte austauschen:

  - **Liste der Unterrichtsfächer**. Einträge der Liste bestehen aus: Name, Beschreibung, Designangaben (Bild, Hintergrundfarbe), Angabe zu Lehrer und Schule, Passwort, Liste der teilnehmenden Schüler, Liste der verknüpften *Unterrichtsstunden*.

  - **Unterrichtsstunden**. Datenobjekte für Unterrichtsstunden bestehen aus: Name der Stunde, ID, Liste der verknüpften *Unterrichtsmaterialien*

  - **Unterrichtsmaterialien.** Datenobjekte für Unterrichtsmaterialien bestehen aus: Name, Bezeichnung des Materialtyps, ID des verknüpften Kurses, ID der verknüpften *Unterrichtsstunde*. Optional: Datei, Link, Beschreibung, Startdatum, Abgabedatum, Verknüpfung mit einer *Umfrage*, auf „privat“ geschaltet

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

- **Umfragen**. Datenobjekte für Umfragen bestehen aus: ID des verknüpften *Unterrichtsmaterial*, Frage, Antwortmöglichkeiten

- **Melden**. Wenn sich ein Schüler über die „Melden"-Funktion im Unterricht aufzeigt, werden verarbeitet: ID der verknüpften *Unterrichtsstunde*, übermittelte Nachricht (optional)

- Lehrer haben die Möglichkeit, sämtliche Dateien zu löschen, welche auf den Tablets während des Unterrichts angefallen sind. Es wird empfohlen, bei Tablets, welche in der Schule verbleiben und nicht schülerbezogen ausgehändigt wurden, jedes Mal am Ende des Unterrichts von dieser Möglichkeit Gebrauch zu machen.

(b) Fernunterricht

Soll Classroom Manage für die Durchführung von Fernunterricht genutzt werden, wird die Verbindung und Datenübertragung zwischen den Endgeräten über eine Cloudinfrastruktur realisiert. Zu diesem Zweck wurden durch den Hersteller der App Tabnova Cloud-Kapazitäten von der Hetzner Online GmbH angemietet. Die für die Übertragung erforderliche Software werden durch Tabnova auf der Infrastruktur von Hetzner betrieben. Der erforderliche Auftragsverarbeitungsvertrag zwischen der Schule bzw. dem Schulträger und Tabnova kann elektronisch im Admin-Bereich des App abgeschlossen werden. Landes- oder schuleigene Big-Blue-Button-Server lassen sich in die App einbinden oder auf in der bereitgestellten Cloud-Infrastruktur betreiben.

Wird die Cloud-Anbindung von Classroom Manage genutzt, werden zusätzlich die folgenden Datenkategorien verarbeitet:

- **Erforderliche Stammdaten:**
  E-Mail, Passwort, ID der Schule (zur Schule werden verarbeitet: Name, Website, Telefonnummer, Daten zu Erstellung/Änderung/Löschung), Datum der Erstellung des Accounts, letzte Änderung, vorgesehene Löschfrist, Rolle (Schüler, Lehrer, Admin), eigenes Profilbild (optional) – *Diese Daten werden zum Zweck der Registrierung und Zugangsverwaltung erhoben und verarbeitet*

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

- **Nutzungsdaten**:
  LDAP-Daten, Zeitzone, Device-Token, IP-Adresse, Big Blue Button Video-Daten (Server kann über die Classroom Manage Cloud betrieben werden oder Einbindung des von den Bundesländern betriebenen Servers der Schulen). – *Diese Daten werden benötigt für Zwecke der Authentifizierung, Anmeldung beim Server und zur Abwicklung der technischen Interaktionen.)*

- **Pädagogische Prozessdaten**: Siehe oben.

In beiden Modi haben Lehrer die Möglichkeit, sämtliche Dateien zu löschen, welche auf den Tablets während des Unterrichts angefallen sind. Es wird empfohlen, bei Tablets, welche in der Schule verbleiben und nicht schülerbezogen ausgehändigt wurden, jedes Mal am Ende des Unterrichts von dieser Möglichkeit Gebrauch zu machen.

3.3. Samsung Produkte/Lösungen

Die zentrale Verwaltung von mobilen Endgeräten in Schulen, Lehranstalten, Ausbildungsstätten und anderen Organisationen, bezüglich Konfiguration, Verteilung der Apps und Wartung der Tablets erfolgt über die Mobile Device Management-Lösung (MDM) Knox Manage oder eines anderen MDM-Dienstleisters wie SOTI MobiControl, Relution o.ä.[4] entweder durch die Schule selbst oder einen Dienstleister.

- **Erforderliche Stammdaten**:
  Um ein mobiles Gerät (Tablet, Smartphone) im MDM verwalten zu können, muss ein entsprechender Benutzer mit eindeutiger Benutzer-ID angelegt werden. Dafür verknüpft man im Regelfalle eine E-Mail-Adresse mit dem Benutzer-Profil im MDM. Dabei kann es sich auch um eine anonyme Adresse handeln, z.B. "Physikraum2@schulname.de", wenn das Tablett nicht einem Schüler fest zugewiesen werden soll. Der Benutzer kann dann im MDM zentral verwaltet werden, entsprechend der sicherheitsrelevanten Konfigurationen für seinen Einsatz.

- **Nutzungsdaten:**
  Seriennummer, IMEI

[4] https://www.samsungknox.com/de/it-solutions/supported-mdm-vendors

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Für die technische Verwaltung der Geräte ist deren Seriennummer bzw. die IMEI erforderlich. Außerdem ist über das Mobile Device Management ein umfassender Zugriff auf technische Parameter und Daten der Tablets möglich. Diese können auch als personenbezogene Daten zu bewerten sein, wenn ein Tablet einer Person eindeutig zugeordnet werden kann, weil die Geräte den Schülerinnen oder Schülern gehören oder weil die Tablets den Schülern fest zugewiesen sind. Weiter unten beschreiben wir, wie die Verantwortliche oder der IT-Dienstleister der Schule die Geräteverwaltung mit datenschutzfreundlichen Grundeinstellungen DSGVO-konform vornehmen können.

3.4. Zusammenfassung der Einsatzmöglichkeiten von **Samsung Neues Lernen**

Die Schule erwirbt Tablets entweder über einen Systemintegrator, Distributor oder Telekommunikationsanbieter. Im nächsten Schritt werden die Tablets von dem jeweiligen Partner über eines der folgenden Szenarien ausgerollt.

Variante a) Konfiguration ausschließlich mit Knox Configure (KC)

Variante b) Registrierung mit Knox Mobile Enrollment und Management mit MDM-System, z.B. Knox Manage (KM)

Variante c) Registrierung mit Knox Mobile Enrollment und Management mit MDM-System, z.B. Knox Manage. Zusätzlich wird Knox Configure genutzt, um z.B. ein individuelles Boot-Logo zu laden.

Schüler erhalten die Geräte dann in einem Zustand, in dem die Sicherheits-Voreinstellung (s.u. VI. Nr. 4 ff.) bereits angewendet wurden und die o.g. Apps (Samsung Classroom Management-App und EduCAP-App) auf die Geräte ausgespielt wurden.

Lehrer können die Geräte der Schüler über die Klassensatzsteuerung in der Samsung Classroom Management-App steuern. Die Classroom Management-App ermöglicht die Durchführung von Fernunterricht. Wird diese Option genutzt, wird der Datenaustausch über eine Cloud-Infrastruktur abgewickelt, die durch den Hersteller der App Tabnova bei der Hetzner Online GmbH angemietet wurden. Es handelt sich dabei um ein deutsches Unternehmen mit Serverstandorten innerhalb Europas.

Bei der erstmaligen Inbetriebnahme der EduCAP-App gibt der Schüler die Edu-ID ein.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

4. Rechtsgrundlage

Für die Verarbeitung von personenbezogenen Daten gilt ein sog. Verbot mit Erlaubnisvorbehalt. Dies ist der Rechtmäßigkeitsgrundsatz des Art. 5 Abs. 1 a) DSGVO. Vom Grundgedanken her ist die Verarbeitung personenbezogener Daten zunächst also unzulässig, es sei denn, dies ist (ausnahmsweise) erlaubt. Dies gilt also auch für die Verarbeitung von Daten über Schüler oder Lehrer durch eine Schule oder den Schulträger. Die erforderliche Rechtsgrundlage lässt sich wie folgt herleiten:

Für die unter Abschnitt III. beschriebenen Verarbeitungstätigkeiten ist zunächst die VO (EU) 2016/679 des Europäischen Parlament und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtline 95/46/EG (Datenschutz-Grundverordnung, DSGVO) zu beachten. Diese steht in der Normenhierarchie als Europäische Verordnung zunächst über den einzelnen Gesetzen der Mitgliedsstaaten, welche ihrerseits über den Gesetzen ihrer Föderalstaaten - im Falle der Bundesrepublik die Bundesländer - stehen. Da der europäische Gesetzgeber mit seiner Gesetzgebung nicht sämtlichen Bereichen des öffentlichen Lebens in allen Mitgliedstaaten gerecht werden kann, hat er in Art. 6 Abs. 1 e) DSGVO i.V.m. Art. 6 Abs. 3 S. 1 b) DSGVO Öffnungsklauseln geschaffen, über welche die Mitgliedstaaten für bestimmte Bereiche des öffentlichen Lebens speziellere Gesetze erlassen können, die dann Anwendungsvorrang gegenüber den in der Normenhierarchie über ihnen stehenden EU-Verordnungen genießen. Dies sind beispielsweise die Schulgesetze und Schuldatenschutzgesetze, sowie die hierzu erlassenen Rechtsverordnungen der einzelnen Bundesländer, sofern sie mit der DSGVO in Einklang zu bringen sind. In einigen Bundesländern und Schultypen können zusätzlich die Landesdatenschutzgesetze und/oder das Bundesdatenschutzgesetz (BDSG) anwendbar sein.

5. Gesetzliche Pflichten

Bei der Durchführung der geplanten Verarbeitung im Zuge von **Samsung Neues Lernen** sind deshalb einige Pflichten zu beachten. Im Einzelnen sind dies die folgenden:

5.1. Pflichten im Zuge der Auftragsverarbeitung

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Antares und Samsung sind an den in diesem Datenschutzkonzept beschriebenen Verarbeitungen von Daten als externe Dritte beteiligt. Wenn die Classroom Manage-App für den Fernunterricht genutzt werden soll, trifft dies wegen der dafür erforderlichen Cloud-Infrastruktur ebenso auf Tabnova zu. Dies geschieht auf Weisung der Verantwortlichen. Daher liegt eine Auftragsverarbeitung nach Art. 28 DSGVO vor.

Nach der DSGVO muss der für die Auftragsverarbeitung Verantwortliche mit dem Auftragnehmer einen Auftragsverarbeitungsvertrag abschließen. Dieser muss auch Regelungen zu den getroffenen technischen und organisatorischen Maßnahmen (TOMs), z. B. zur Datensicherung und zur Gewährleistung der Vertraulichkeit, enthalten.

Die oben genannten Auftragsverarbeiter stellen Ihnen solche Auftragsverarbeitungsverträge zur Verfügung, mit denen Sie nachweisen können, dass Sie

- die Auftragsverarbeiter sorgfältig ausgewählt haben,
- die Auftragsverarbeiter adäquate TOMs zum Schutz der weitergegebenen Daten anwenden und
- diese adäquaten TOMs seitens der Auftragsverarbeiter ausreichend dokumentiert werden.

Diese Unterlagen haben Sie im Zuge des Vertragsschlusses oder während des Einrichtungsprozesses übermittelt bekommen. Sie sind sorgfältig aufzubewahren und erforderlichenfalls vorzulegen.

5.2. Allgemeine Datenschutzanforderungen

Datenschutz ist nicht nur ein technisches Thema. Für einen wirksamen Datenschutz in Schulen sind eine Sensibilisierung und Schulung der Lehrer und der weiteren Mitarbeiter ebenfalls erforderlich. Nur wenn Datenschutz fest in der täglichen Arbeit und im Unterricht verankert ist, wird es gelingen, die wachsende Digitalisierung mit der Einhaltung der Pflichten aus der DSGVO in Einklang zu bringen. Dabei muss sich der Datenschutz nicht zu einem bürokratischen Hindernis entwickeln. Vielmehr lässt sich eine pragmatische und konstruktive Lösung erarbeiten, welche die gesetzlichen Auflagen erfüllt.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Alle Mitarbeiter der Schule, welche Umgang mit personenbezogenen Daten haben, sind auf einen vertraulichen Umgang mit diesen Daten verpflichtet. Deshalb sollten alle Mitarbeiter zur Sensibilisierung in regelmäßigen Abständen Datenschutzschulungen erhalten, insbesondere in Bezug auf die im Unterricht eingesetzten EDV-Anlagen. Zu diesem Zweck steht die secjur GmbH gerne als Partner an der Seite der Schulen.

Zur Sensibilisierung des Lehrerkollegiums und aller weiteren Angestellten schlagen wir folgende Maßnahmen vor:

- Verpflichtung eines jeden Mitarbeiters auf den Datenschutz
- Teilnahme an regelmäßigen Datenschutzschulungen
- Passwortrichtlinie innerhalb der Schule (s.u. XI Nr. 1)
- Erstellung eines Berechtigungskonzeptes in Bezug auf die verwendeten Systeme (für die vorliegenden Systeme s.u. XI. Nr. 2)
- Erstellung einer Dienstanweisung zur getrennten Nutzung von Internet/ E-Mail (privat/geschäftlich)
- Erstellung einer Dienstanweisung zur getrennten Nutzung von Handys/ Laptops/ und beweglicher Hardware (privat/dienstlich)
- Bereitstellung von Orientierungshilfen an sämtliche an der gegenständlichen Verarbeitung beteiligten Mitarbeiter/-innen

Einige der oben genannten Anforderungen können erfüllt werden, indem den Empfehlungen dieses Datenschutzkonzeptes gefolgt wird und zum Beispiel die Vorlagen aus der Anlage genutzt werden.

5.3. Technische- und organisatorische Maßnahmen (TOMs)

Der Datenschutz erfordert neben einem verantwortungsvollen Umgang mit den materiellen Anforderungen (Rechtsgrundlage, Erforderlichkeit, Zweckbindung, Datenvermeidung etc.) innerhalb der datenverarbeitenden Stelle auch die Verwendung einer sicheren und gegen

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Angriffe von nicht berechtigten Dritten geschützten IT-Infrastruktur. Die Schule muss deshalb bei der Durchführung von digitalen Lehrmethoden TOMs implementieren, um das benötigte Maß an Vertraulichkeit, Verfügbarkeit und Integrität der zu verarbeitenden Daten der Lehrenden und Lernenden sicherzustellen (angemessenes Schutzniveau).

Datenschutz betrachtet die Maßnahmen der Informationssicherheit als wesentliches Werkzeug, um Datenschutzziele zu erreichen. Gemäß Art. 32 DSGVO ist die Einhaltung bestimmter TOMs zwingend.

Um technische und organisatorische Maßnahmen hinsichtlich ihrer Angemessenheit bewerten zu können, ist es erforderlich, das Schadenspotential (d.h. den Grad möglicher Beeinträchtigung schutzwürdiger Belange) näher zu bestimmen. Hierzu kann ein Schutzstufenkonzept erstellt werden.

Anerkannt ist das Schutzstufenkonzept der Aufsichtsbehörde aus Niedersachsen[5] mit fünf Schutzstufen, welches Schulen zur Definition des angemessenen Schutzniveaus anwenden können:

Stufe	Personenbezogene Daten...	Beispiele
A	...welche frei zugänglich sind.	Telefonbücher, Adressbücher, Wahlvorschlags-verzeichnisse
B	...deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch zumindest an ein berechtigtes Interesse der Einsichtnehmenden gebunden sein muss.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen
C	...deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte (“Ansehen").	Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten

[5] https://lfd.niedersachsen.de/startseite/technik_und_organisation/schutzstufen/schutzstufen-56140.html

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

D	...deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte (“Existenz”).	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Gesundheitsdaten, Schulden, Pfändungen
E	...deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können.

In den allermeisten Fällen können die bei dem hier gegenständlichen Projekt **Samsung Neues Lernen** verarbeiteten personenbezogenen Daten den Schutzstufen B und C zugeordnet werden. Zur Umsetzung der IT-Sicherheit für diese Daten dienen die in den Handreichungen "IT-Grundschutz" des BSI genannten Empfehlungen gemäß welchen das Risiko im Allgemein als gering einzuschätzen ist.

Ausnahmen ergeben sich beispielsweise in Fällen, in welchen die verarbeiteten Bearbeitungsstände zu einem gewichtigen Anteil in die Endnote der Schüler eingehen (also bspw. bei einer Klassenarbeit, nicht aber z.B. einer einzelnen Note für soziale Mitarbeit in Bezug auf eine Unterrichtsstunde), kann nach unserem Dafürhalten davon ausgegangen werden, dass die Schutzstufe D in Einzelfällen einschlägig sein könnte.

Eine Schutzstufenklassifizierung allein reicht allerdings nicht aus, um daraus direkt die erforderlichen und angemessenen technischen-organisatorischen Maßnahmenempfehlung abzuleiten.

Für die Erstellung einer angemessenen technisch-organisatorischen Maßnahmenempfehlung ist das Schadenspotential einer Gefährdung im Rahmen einer Gefahren- und Risikoanalyse gemeinsam mit deren Eintrittswahrscheinlichkeit zu bewerten. Erst hieraus lassen sich bestimmte Schutzbedarfskategorien/Risikobereiche entwickeln, für die adäquate Sicherheitsmaßnahmen definiert werden können. Eine entsprechende Risikobewertung wird anhand der untenstehenden Matrix vorgenommen.

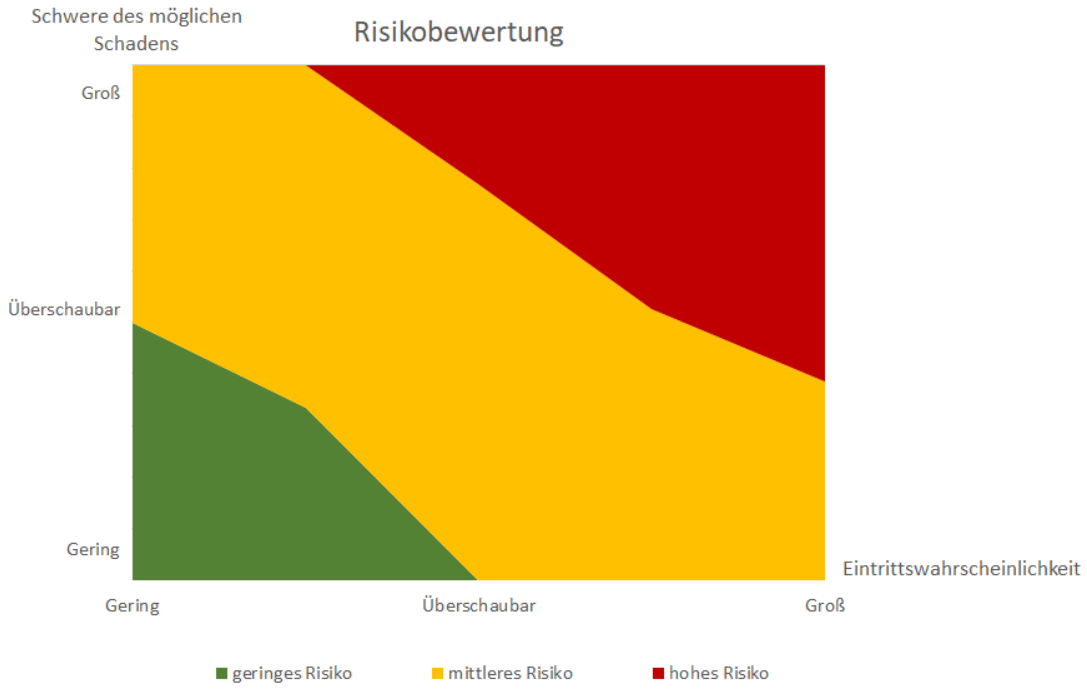
secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl



(a) Bestimmung möglicher Schäden

Zur Bestimmung des angemessenen Schutzniveaus müssen zunächst mögliche Schäden für die Rechte der Betroffenen (hier insb. der Schüler) definiert werden. Mögliche Schäden sind in Erwägungsgrund 85 zur DSGVO genannt. Dies sind etwa der Verlust der Kontrolle über personenbezogenen Daten oder Einschränkung der Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

Vorliegend kommt ein möglicher Schaden vornehmlich in Gestalt von gesellschaftlichen Nachteilen der Schüler in Betracht. Beispielhaft wäre eine für den jeweiligen Schüler nachteilige Veränderung der eingegebenen Lernstandkontrollen denkbar, welche dann Gegenstand von negativen Leistungsbewertungen werden könnten. Als Resultat negativer Leistungsbewertungen ist es beispielsweise möglich, dass ein Schüler nicht in die nächste Jahrgangsstufe versetzt wird und dadurch gesellschaftliche Nachteile erleidet.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

(b) Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden

Weiter müsste das definierte Risiko aber auch eine gewisse Schwere aufweisen und dürfte nicht unterhalb einer Bagatellgrenze liegen. Die Überschreitung einer Erheblichkeitsschwelle ist zumindest für die hypothetische Fälle unseres Beispiels zu bejahen.

Somit kann im Einzelfall nicht ausgeschlossen werden, dass es bei einer unbefugten Veränderung der Lernstandkontrollen zu einem persönlichen Nachteil des betroffenen Schülers kommen kann, welcher über der Erheblichkeitsschwelle liegt. Da eine Nichtversetzung weitreichende Konsequenzen (nach wiederholtem Male sogar Beendigung der Schullaufbahn) zeitigen kann, ist von einer substanziellen Schwere des möglichen Schadens auszugehen.

Hinsichtlich der Eintrittswahrscheinlichkeit sind die systemseitigen Gestaltungsmöglichkeiten zu berücksichtigen.

Um das Ergebnis vorweg zu nehmen, bewerten wir die Eintrittswahrscheinlichkeit des o.g. Schadens mit “vernachlässigbar”, sofern den vor dem Hintergrund der vorgenannten Erwägungen im folgenden Abschnitt ausgesprochenen Konfigurationsempfehlungen gefolgt wird.

6. Konfigurationsempfehlungen

Samsung Knox stellt verschiedene Sicherheitsfunktionen zur Verfügung. Generell wird empfohlen, möglichst alle verfügbaren optionalen Knox-Sicherheitsfunktionen zu aktivieren, sofern hierfür die nötigen Lizenzen erworben wurden. Um den Anforderungen des konkreten Einzelfalles gerecht zu werden, gehen wir im Folgenden etwas in die Tiefe, lassen jedoch bewusst einige Punkte unerwähnt, welche wir für den beschriebenen Sachverhalt als unverhältnismäßig erachten. Die Datenflüsse der vorgenannten Verarbeitungen haben wir unter III dargestellt. Bei der Planung der Verarbeitung von personenbezogenen Daten sind immer auch die Grundsätze („Privacy by Design“) und („Privacy by Default“) zu berücksichtigen. Nach den Grundsätzen Datenschutz durch Technikgestaltung („Privacy by Design“) und durch datenschutzfreundliche Voreinstellungen („Privacy by Default“) muss die betroffene Person darauf vertrauen können, dass die grundsätzlichen

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Datenschutzanforderungen von der ersten Nutzung an gewahrt bleiben, und zwar auch dann, wenn die vorgegebenen Voreinstellungen zunächst nicht geändert werden. Diese Anforderung gehört zu einem der Kernelemente der DSGVO. Ziel des „Privacy by Default"-Grundsatzes ist es, dass Verantwortliche nur Systeme bereitstellen, deren Voreinstellungen bereits möglichst datenschutzfreundlich sind.

Vor dem Hintergrund dieses Grundsatzes und um dem o.g. Risiko der möglicherweise einschlägigen Schutzstufe D gerecht zu werden, haben wir die folgenden Voreinstellungsempfehlungen erstellt, die von der Verantwortlichen vor Aushändigung der Geräte an Betroffene vorgenommen werden sollen:

6.1. Vereinfachte Passwortrichtlinie

Die Nutzung einer Online-Lernplattform erfordert nach Ansicht der Datenschutzkonferenz (DSK) der Länder einen passwortgeschützten Zugriff. Die Vorgabe muss grundsätzlich umgesetzt werden. Hinsichtlich der Antares Produkte ist jedoch festzustellen, dass diese keine vollwertige Online-Lernplattform darstellen, sondern lediglich eine Art „Mediathek mit Freigabefunktion" mit der Möglichkeit einige Lernstandkontrollen (Lückentexte und Multiple-Choice-Tests) durchzuführen. Ähnlich verhält es sich bei der Classroom Management App, die primär den Austausch von Dateien und die Durchführung des Unterrichts unterstützt.

Um den Anforderungen der Praxis gerecht zu werden, haben wir diese in einer vereinfachten Form dargestellt:

- Passwörter sind aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen zusammenzusetzen.

- Passwörter müssen eine Mindestlänge von 8 Stellen aufweisen. (Hiervon kann im Einzelfall aufgrund von Alter nach unten abgewichen werden, um keine Zugangshindernisse zu schaffen. Eine Mindestlänge von 6 Zeichen sollte nach Möglichkeit aber nicht unterschritten werden)

- Passwörter, die leicht zu erraten sind oder in einem Sinnzusammenhang stehen, sind nicht zulässig.

- Passwörter sind während der Eingabe am Bildschirm nicht lesbar.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

- Benutzerkonten sind nach 4-maliger Falscheingabe automatisch zu sperren.
- Benutzerkonten sind nach 90 Tagen Inaktivität automatisch zu sperren.
- Am Ende eines jeden Schuljahres ist ein Wechsel der Passwörter durchzuführen.
- Passwörter sind nach dem jeweiligen Stand der Technik verschlüsselt zu speichern.
- Passwörter dürfen nur verschlüsselt im Netzwerk übertragen werden.
- Anwender sind darauf zu verpflichten, das Passwort geheim zu halten. Die Passwörter dürfen nicht unverschlüsselt auf dem Rechner oder offen auf dem Arbeitsplatz hinterlegt werden (etwa auf einem Klebezettel). Die Eingabe des Passwortes muss geheim erfolgen.

Insgesamt halten wir es für vertretbar, beim Einsatz der Passwortrichtlinie hinsichtlich der Schüler Ausnahmen in dem Fall zu machen, dass die Schüler ständig ein individuelles Gerät nutzen (BYOD), welches von diesen selbst mit Zugangsbeschränkungen versehen wurde. Ansonsten sollte vom Einsatz einer Passwortrichtlinie nicht abgesehen werden.

6.2. Rollen- und Zugriffskonzept

Für die einzelnen Komponenten von **Samsung Neues Lernen** sind zur Minimierung der Zugriffsmöglichkeiten auf personenbezogene Daten folgende Rollen mit den beschriebenen Berechtigungen vorgesehen.

- **Administratoren.** Administratoren haben alle Berechtigungen für sämtliche Einstellungsmöglichkeiten, sowohl für Nutzerkonten als auch für das Gesamtsystem **Samsung Neues Lernen**, der Konfiguration der Tablets und der Installation notwendiger Apps. Grundsätzlich liegen die Administratoren-Berechtigungen bei der Schule, um alle unten beschriebenen datenschutzfreundlichen Grundeinstellungen und die Verwaltung der Schüler- und Lehrertablets durch die Schule selbst vorzunehmen. (Zum Beispiel durch eine Kollegin oder einen Kollegen mit entsprechender Funktionsstelle.) Wenn die IT-Administration der Schule extern vorgenommen wird, etwa durch eine zentrale Stelle des Landes oder einen Dienstleister (Systemhaus bzw. Reseller), kann die Schule den Zugriff auf die Tablets

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

an diese Stelle freigeben, indem sie diesen einen Account als sogenannten *Sub-Administrator* erstellt.

- **Medienzentren.** Die Medienzentren der Länder verwalten die Lerninhalte, die für eine Schule lizenziert wurden und auf die mit der EduCAP-App oder über EduPool zugegriffen werden kann. Sie haben die Befugnis, Accounts mit der Rolle "Lehrer" und "Schuladministrator" anzulegen. Zugriff auf personenbezogene Daten haben diese im Übrigen nicht.

- **Schuladministratoren**. Um den Verwaltungsaufwand der Medienzentren zu verringern, können Schulen das Anlegen der Lehrer-Accounts auch selbst übernehmen. Dafür kann der Schule ein Account mit der Rolle "Schuladministrator" zugewiesen werden.

- **Lehrer**. Lehrer haben mittels der Samsung Classroom Management App zum Zwecke des Classroom Managements Berechtigungen, die Unterrichtsstunden anzulegen und zu verwalten. Ferner haben sie die technische Berechtigung, über den Austausch von Daten mittels der App zu bestimmen oder auf den Tablets der Schüler den Bildschirm zu sperren. Unter EduPool/EduCAP können Lehrkräfte Accounts für Schüler erstellen, indem sie in einer entsprechenden Nutzeroberfläche eine Liste von Edu-IDs für ihre jeweilige Klasse erstellen. Lehrer können für eine Klasse digitale Lerninhalte freigeben, für die die Schule zuvor Lizenzen erworben hat. Lehrer können außerdem die Ergebnisse der Auswertungsbögen der Schüler über ihre jeweilige Edu-ID einsehen.

- **Schüler**. Schüler können mit den Inhalten arbeiten, die für sie freigegeben wurden. Sie können Eingaben tätigen, etwa Auswertungsbögen ausfüllen, Dateien an den Lehrer schicken, Dateien empfangen und bearbeiten, am (Fern-)Unterricht teilnehmen oder sich elektronisch mit einer Nachricht melden.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

6.3. Knox Configure

Mit Knox Configure haben Verantwortliche (Schule oder Schulträger) die Möglichkeit, die Geräteeinstellungen der erworbenen Tablets zu konfigurieren (siehe Enrollment-Szenario a) und c) in Abschnitt III Nr. 4). Wir empfehlen folgende Maßnahmen zum Datenschutz durch Technikgestaltung:

Lfd. Nr.	Option	Empfehlung	Begründung
#01 KC	Anlegen eines Konfigura-tionsprofils	A) Unter dem Punkt "Profile" lassen sich ebenjene für die in Rede stehenden Tablets anlegen. Hier gibt es die Gelegenheit, eine zusätzliche Datenschutzerklärung einzufügen, welche die Nutzer vor Inbetriebnahme des Gerätes einsehen können. Hier kann die (unter Kapitel 8) in den Anlagen mitgelieferte Datenschutzerklärung einfügt werden. B) Weiter sollte die Option „den Einrichtungsassistenten überspringen und FRP-Umgehung aktivieren" ausgewählt werden.	A) Nach Art. 13 DSGVO treffen den Verantwortlichen bestimmte Informationspflichten bei der Erhebung von personenbezogenen Daten bei der betroffenen Person. Um die Einhaltung dieser Pflichten sicherzustellen, ist es empfehlenswert, diese Informationen über das System bei Inbetriebnahme des Gerätes zur Verfügung zu stellen. B) Nach dem Grundsatz Privacy by Default sind die datenschutzfreundlichsten Grundeinstellungen zu wählen, mit denen der gewünschte Zweck (s.o. in der Einleitung) erreicht werden kann. Durch das Überspringen der Einrichtungsbildschirme wird verhindert, dass das Gerät auf das private Google-Konto des Schülers festgelegt wird und dieser dann einerseits von Google identifiziert werden kann und andererseits das Zurücksetzen des Geräts aufgrund der privaten „Factory Reset Protection" für den Administrator der Schule gesperrt ist.
#02 KC	Pro-Kiosk oder Normalmo-dus	Im Pro-Kiosk-Modus kann beispielsweise eingestellt werden, dass das Gerät nur mit einer bestimmten App betrieben werden kann, oder der Nutzer sich ausschließlich auf einer bestimmten URL-Domäne bewegen kann. Wir empfehlen	Diese Maßnahmen werden nur empfohlen, sofern sie die operativen Abläufe nicht stören. Sie dienen ebenfalls der Gewährleistung der Systemintegrität gem. Art. 32 DSGVO.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

		hiervon Gebrauch zu machen, sofern die Geräte in einem bestimmten Anwendungsfall nur mit einer einzigen Anwendung betrieben werden.	
#03 KC	Start- und Sperr-bildschirm	Wir empfehlen, sämtliche Widgets auszublenden, die nicht dem Zweck der Durchführung des Unterrichts dienen. Diese sind: • Uhrzeit • Datum • Besitzerinformationen • Benachrichtigungen • Hilfetext • Shortcuts Einzig die Akkuinformationen sollten sie eingeblendet lassen, damit die Geräte rechtzeitig aufgeladen werden können.	Nach Art. 32 DSGVO sind geeignete technische und organisatorische Maßnahmen zu veranlassen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies beinhaltet Maßnahmen, welche die Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen sollen. Aufgrund der experimentierfreudigen Natur der Digital-natives sollte deshalb jedes mögliche Risiko für Manipulationen an Systemen minimiert werden, unabhängig davon, wie banal es erscheinen mag.
#04 KC	Ton und Anzeige	Sofern ein Einsatz der Geräte im Kiosk-Modus geplant ist, sollten Sie das Ausblenden der Systemleiste in Erwägung ziehen. Diese Option steht im Bereich “Ton und Anzeige” zur Verfügung.	Diese Maßnahme wird nur empfohlen, sofern sie den operativen Ablauf nicht stört. Sie dient ebenfalls der Gewährleistung der Systemintegrität.
#05 KC	Anwendungen und Inhalt	Es wird empfohlen: • Alle vorinstallierten Browser zu deaktivieren • Den Google Play Store zu deaktivieren • S Voice zu deaktivieren Für den Anwendungsfall „Pro-Kiosk“ (s. #02KC) kann an dieser Stelle sichergestellt werden, dass die schulrelevante App bei einem Neustart des Gerätes automatisch startet.	Gem. Art. 6 DSGVO ist die Verarbeitung von personenbezogenen Daten nur rechtmäßig, wenn eine entsprechende Rechtsgrundlage zur Verfügung steht. Durch den Chrome Browser und den Playstore werden bestimmte personenbezogene Daten an Google übertragen. Obwohl Google hierfür zunächst eine Einwilligung des Betroffenen einholt, ist die Rechtmäßigkeit der hierauf basierenden Einwilligung wegen der bei einigen Schülern gegebenen, mangelnden Einsichtsfähigkeit in die Tragweite dieser Einwilligung kritisch zu sehen. Vor dem Hintergrund des Privacy by Design-Grundsatzes sind

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

		Hinweis für Schuladministratoren: An dieser Stelle lassen sich auch URLs auf die Blacklist setzen, was etwa erforderlich sein kann, um Anforderungen des Jugendschutzes gerecht zu werden. Zu dieser Maßnahme raten wir, sofern nicht alle voreingestellten Browser entsprechend unserer Empfehlung deaktiviert werden.	durch den Verantwortlichen Maßnahmen zu treffen, die eine möglichst datenschutzfreundliche Grundkonfiguration darstellen. Dieser Anforderung kann der Verantwortliche gerecht werden durch die Verhinderung von nicht dem Verarbeitungszweck des Gegenstandes dieses Datenschutzkonzept dienenden Verarbeitungstätigkeiten.
#06 KC	Gerätekonnektivität	An dieser Stelle lässt sich das Schul-WLAN als automatisches Heimnetz definieren. Dies wird erforderlich sein, sofern der Verantwortliche der Empfehlung folgt, die Systemleiste zu deaktivieren. Weiter wird geraten, den Sichtbarkeitsmodus von Bluetooth zu deaktivieren. Mobile Daten und die NFC-Schnittstelle sollten ebenfalls deaktiviert werden.	Diese Maßnahmen werden nur empfohlen, sofern sie die operativen Abläufe nicht stören. Sie dienen ebenfalls der Gewährleistung der Systemintegrität gem. Art. 32 DSGVO.
#07 KC	Geräte-einstellungen	Unsere Empfehlung ist, folgende Einstellungsmenü-Elemente auszublenden: • Sichern und Zurücksetzen • Bluetooth • Entwickler • Offline-Modus • Gerätesicherheit (Sperrbildschirm) • WLAN Weiter empfehlen wir die Aktivierung der Option “Nicht zulassen, dass das Gerät von einer anderen Quelle angepasst wird, nachdem es mit dem Knox Configure angepasst wurde.”	Diese Maßnahmen werden nur empfohlen, sofern sie die operativen Abläufe nicht störten. Sie dienen ebenfalls der Gewährleistung der Systemintegrität gem. Art. 32 DSGVO.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

#08 KC	Beschränkungen	Es sollten folgende Beschränkungen vorgenommen werden: • Verhindern, dass Endbenutzer die Kamera verwenden. • Verhindern, dass Endbenutzer auf das Einstellungsmenü zugreifen. • Verhindern, dass Endbenutzer den zweiten SIM-Kartensteckplatz verwenden • SD-Kartenzugriff deaktivieren. • Media Transfer Protocol (MTP) für USB deaktivieren. • USB-Hostspeicherung deaktivieren.	Diese Maßnahmen werden nur empfohlen, sofern sie die operativen Abläufe nicht störten. Sie dienen ebenfalls der Gewährleistung der Systemintegrität gem. Art. 32 DSGVO.
#09 KC	Sicherheits-einstellungen	Folgende Sicherheitseinstellungen sollten vorgenommen werden: • Fingerabdruck-Scanner deaktivieren • Iris-Scanner deaktivieren • Gesichtserkennung deaktivieren	Gem. Art. 6 DSGVO ist die Verarbeitung von personenbezogenen Daten nur rechtmäßig, wenn eine entsprechende Rechtsgrundlage zur Verfügung steht. Sowohl der Fingerabdruck als auch der Iris-Scanner und die mathematische Erfassung der Gesichtsparameter stellen personenbezogene Daten im Sinne der DSGVO dar. Bereits das Einlesen der entsprechenden Daten (Fingerabdruck, Iris, Gesichtserkennung) stellt eine automatisierte Verarbeitung dar, egal ob diese Daten anschließend übertragen werden oder nicht. Für eine solche Verarbeitung fehlt es vorliegend an einer Rechtsgrundlage.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

6.4. Knox Mobile Enrollment

Mit dieser Lösung können Verantwortliche (bzw. ihre Administratoren) eine Vielzahl an Tablets von Samsung gleichzeitig der Organisation hinzufügen, ohne jedes Gerät einzeln anmelden zu müssen. Der Verantwortliche muss das Gerät nur einschalten und sich beim Netzwerk anmelden, um sich dann beim MDM von Samsung oder deren MDM-Partnern zu registrieren (siehe Enrollment-Szenario b) unter III Nr. 4).

Hinsichtlich Knox Mobile Enrollment empfehlen wir, folgende Hinweise zu beachten:

Lfd. Nr.	Option	Empfehlung	Begründung
#01 KME	Geräte	Sichtbar sind insbesondere die IMEI bzw. Serien-Nummern. Diese sind nur im BOYD-Szenario oder im Falle einer festen Zuweisung der Geräte als personenbezogene Daten zu klassifizieren. Wir empfehlen jedoch in jedem Fall, den Zugang zu Knox Mobile Enrollment auf die erforderlichen Rollen aus dem Berichtigungskonzept [s.o.] zu begrenzen.	Nach Art. 32 DSGVO sind geeignete technische und organisatorische Maßnahmen zu veranlassen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies beinhaltet auch eine Begrenzung der Systemadministratoren auf ein erforderliches Minimum. Der größte Risikofaktor für Systeme ist der Mensch. Im Falle des Systemadministrators sogar ganz besonders, da dieser den größten Schaden anrichten kann. Systemadministratoren sollten vor diesem Hintergrund auch sorgsam ausgewählt werden und über die nötige Redlichkeit verfügen. In Einzelfällen kann es deshalb sogar angezeigt sein, nur solche Personen zum Administrator zu machen, welche über ein einwandfreies polizeiliches Führungszeugnis verfügen.
#02 KME	MDM-Profile	Hier können Profile für das automatische Ausrollen der Geräte erstellt werden bis hin zur MDM-Aktivierung. Dies wird empfohlen. Dies kann erreicht werden, indem der MDM-Agent mittels eines APK-Download-Links auf die Geräte installiert und ausgeführt wird.	Ein MDM dient der Aktivierung, Verwaltung und Absicherung von mobilen Systemen der Schule, auch wenn es sich um private Geräte der Schülerin oder des Schülers handelt. Nach Art. 32 DSGVO sind geeignete technische und organisatorische Maßnahmen zu veranlassen, um ein dem Risiko angemessenes

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

		Damit sich das Gerät beim entsprechenden MDM System melden kann, muss unter dem Punkt “MDM Profiles” die URI (Server-URL des MDM Systems) hinterlegt werden. Weiter empfehlen wir für Android Enterprise, ein Device-Owner-Profil zu konfigurieren, welches keinen Personenbezug enthält, z.B. „Pestalozzi-Schule“, oder „Klasse-6B“.	Schutzniveau zu gewährleisten. Die Verwendung einer Lösung zur Aktivierung, Verwaltung und Absicherung von mobilen Endgeräten dient der Standardisierung und damit der besseren Kontrolle.
#03 KME	Einzel-händler	An dieser Stelle kann die Einzelhändler-ID mit der Knox-Kunden-ID verknüpft werden und dem Einzelhändler können bestimmte Rechte eingeräumt werden. Beide IDs sind an dieser Stelle im Normallfall keine personenbezogenen Daten. Wir empfehlen, alle von einem Einzelhändler hochgeladenen Geräte automatisch genehmigen zu lassen, da sich diese dann sofort unter der Kontrolle des Systemadministrators befinden.	Diese Maßnahmen werden nur empfohlen, sofern sie die operativen Abläufe nicht stören. Sie dienen ebenfalls der Gewährleistung der Systemintegrität gem. Art. 32 DSGVO.
#04 KME	Geräte-benutzer	Es wird empfohlen, eine allgemeine Benutzer-ID zu vergeben, welche keine Rückschlüsse auf eine natürliche Person als Besitzer zulässt.	Diese Maßnahme dient der Pseudonymisierung iSv. Art. 25 DSGVO. Mit dieser Maßnahme können die Datenschutzgrundsätze wie etwa Datenminimierung möglichst wirksam umgesetzt werden.
#05 KME	Adminis-tratoren und Rollen	Wir empfehlen, die Administratoren entsprechend der erforderlichen Rollen und Funktionen aus dem Berichtigungskonzept [s.o.] zu konfigurieren.	Nach Art. 32 DSGVO sind geeignete technische und organisatorische Maßnahmen zu veranlassen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies beinhaltet auch eine Begrenzung der Systemadministratoren auf ein erforderliches Minimum.
#06 KME	Aktivitäts-protokoll	An dieser Stelle lässt sich einsehen, welcher Login-Name zu welchem Zeitpunkt welche Tätigkeit ausführte.	Durch die Dokumentation kann nachgewiesen werden, dass der Systemadministrator weiterhin für die Ausführung dieser Rolle geeignet ist.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

		Diese Dokumentation empfehlen wir, regelmäßig vom Systemadministrator im Beisein einer weiteren, neutralen Person einzusehen und abzulegen.	

6.5. MDM-Richtlinie

Mit einem MDM-System (wie Samsung Knox Manage [s.u. Nr. 6]) ist die zentrale Verwaltung von mobilen Endgeräten möglich. Der Administrator kann bspw. Sicherheitsupdates einspielen, Geräte sperren oder Einschränkungen hinsichtlich der auf den Geräten installierbaren Anwendungen vornehmen (Black- oder Whitelists). Auch lassen sich bis zu einem gewissen Grad die laufenden Geräte hinsichtlich ihrer Anwendungen (Befehlsverlauf, E-Mail und SMS-Verlauf, Geräteprotokoll) und ihres Standortes überwachen.

Mit diesen weitreichenden Berechtigungen der Administratoren müssen diese verantwortungsvoll umgehen. Die Verhältnismäßigkeit und der Schutz der Persönlichkeitsrechte der betroffenen Personen müssen stets gewährleistet sein. Der Schul-Admin darf beispielsweise das geschriebene Wort der Schüler weder abhören noch aufzeichnen. Eine unbegründete Überwachung verstößt gegen die gesetzlich geregelte Vertraulichkeit des Wortes (§ 201 Strafgesetzbuch). Der Administrator ist ferner darauf (dienstrechtlich) zu verpflichten, das MDM-System ausschließlich zum Zweck der Gerätewartung, Konfiguration und Prozessoptimierung zu nutzen.

6.6. Knox Manage

Sofern der Verantwortliche sich für die MDM-Lösung von Knox (Knox Manage, KM) entschieden hat, hat er die Gelegenheit, Schüler- und Lehrertablets im pädagogischen Schulnetzwerk (optional Knox Container mit Zwei-Faktor-Authentifizierung) zu verwalten (siehe Enrollment-Szenario b) und c) unter III Nr. 4).

Wenn der Nutzerzugang angelegt wird, ist unbedingt darauf zu achten, die Region der eingesetzten Server so auszuwählen, dass nur Server innerhalb des europäischen Wirtschaftsraumes verwendet werden.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Wir empfehlen folgende Maßnahmen:

Lfd. Nr.	Option	Empfehlung	Begründung
#01 KM	Gerät	Bislang wurde die Seriennummer des Gerätes (bei WLAN Only), bzw. die IMEI bei Geräten mit mobilen Daten übertragen, wenn der „Manage-Type“ auf „Android Legacy“ konfiguriert wurde. Mit der Umstellung des „Manage-Type“ auf „Android Enterprise“ wird dieses nicht mehr erfolgen, was eine weitere Maßnahme der Datensparsamkeit darstellt. Geräte-Aktivierungen in Android Enterprise: Google hat klare Begriffe für die möglichen Aktivierungsszenarien eingeführt: BYOD - Work Profile COBO - Fully Managed COPE – Fully Managed Device with Work Profile BYOD – Private Geräte werden in die Schulumgebung eingebunden und bekommen einen Arbeitsbereich „Work Profile“. Der Administrator hat keinerlei Zugriff auf die privaten Daten, und kann nur den Work Profile- Bereich administrieren. COBO – Schuleigene Geräte werden in die Schulumgebung eingebunden und dienen nur dem Schulbetrieb. Globale IT-Richtlinien lassen sich auf dem Gerät umsetzen. COPE – Schuleigene Geräte werden in die Schulumgebung eingebunden und dienen dem	Nach Art. 32 DSGVO sind geeignete technische und organisatorische Maßnahmen zu veranlassen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies beinhaltet Maßnahmen, welche die Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen sollen. Aufgrund der experimentierfreudigen Natur mancher „Digital Natives“ oder einem allgemeinen jugendlichen Drang, Grenzen auszutesten, sollte deshalb jedes mögliche Risiko für Manipulationen an Systemen minimiert werden, unabhängig davon, wie banal es erscheinen mag.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

		Schulbetrieb und Nutzer dürfen diese auch privat benutzen. Hier können globale IT-Richtlinien durchgesetzt werden! Der Administrator, der das MDM System verwaltet, kann Richtlinien auf den Geräten durchsetzen, wie beispielsweise: • Die Geräteregistrierung aufheben • Lizenz aktualisieren • Knox Manage aktualisieren • Das Gerät auf Werkseinstellungen zurücksetzen • Ein Überwachungsprotokoll erfassen • Ein Geräteprotokoll erfassen • Diagnoseinformationen erfassen Wir empfehlen, Geräte, welche der Schule gehören, auf den Manage-type “Fully Managed” zu setzen. Im Fall von BYOD (Bring-your-own-device) kann der Administrator mit „Work Profile“ einen Arbeitsbereich für den Schuleinsatz zentral verwalten.	
#02 KM	Benutzer	Unsere Empfehlung an dieser Stelle lautet, für alle Usernamen im MDM eine Bezeichnung zu wählen, die keinen Personenbezug zulässt. Also z.B. “Tablet1...” bei Geräten die der Schule gehören. Weiter sollte über den Punkt Benutzer die “Passwortrichtlinie" (s.o. unter VI. 1) durchgesetzt werden. Hinsichtlich der User-Verwaltung empfehlen wir eine E-Mail-Adresse	Diese Maßnahme dient der Pseudonymisierung u.a nach Art. 25 DSGVO. Mit dieser Maßnahme können die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umgesetzt werden.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

		zu hinterlegen, die keine Rückschlüsse auf eine bestimmte Person zulässt. Für die Nutzung der Android Enterprise Leistungsmerkmale im MDM muss bei Google ein Google-Business-Account erstellt werden und im MDM hinterlegt werden. Mobiltelefonnummern (optional) sollten nach unserem Dafürhalten nicht hinterlegt werden.	
#03 KM	Gruppe	An dieser Stelle besteht die Möglichkeit, Gruppierungen in Bezug auf die Organisationseinheiten (s.u. #04KM) vorzunehmen. Beispielsweise können Schüler und Lehrer gruppiert werden und übergeordnet über die Gruppe bspw. die Samsung Classroom Management-App ausgespielt werden, da beide Organisationseinheiten die App benötigen. Oder es können z.B. Lehrer und das Sekretariat gruppiert werden, da beide Einheiten einen E-Mail-Client zur Kommunikation untereinander benötigen.	Diese Maßnahmen werden nur empfohlen, sofern sie die operativen Abläufe nicht stören. Sie dienen ebenfalls der Gewährleistung der Systemintegrität gem. Art. 32 DSGVO.
#04 KM	Organisation	Wir empfehlen im Management der Organisation folgende Ebenen anzulegen: Oberste-Ebene: **Schule** Darunter: **Sekretariat/Verwaltung** Darunter: **Lehrer**	Nach Art. 32 DSGVO sind geeignete technische und organisatorische Maßnahmen zu veranlassen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Verwendung einer Lösung zur Aktivierung, Verwaltung und Absicherung von mobilen dient der Standardisierung und damit der besseren Kontrolle.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

		Darunter: **Schüler** Dies erlaubt dem Systemadministrator die verschiedenen Richtlinien auf die einzelnen Untereinheiten anzuwenden, was eine bessere Kontrolle der eingesetzten Geräte ermöglicht.	
#05 KM	Anwen-dung	Mittels Knox Manage kann eingestellt werden, was aus dem Google-Play-Store heruntergeladen werden kann (Taschenrechner App etc.). Hier empfehlen wir die Konfiguration entsprechend der Schul-Gesamtlösung vorzunehmen. Weiter gibt es in dem Punkt “Anwendungen” die Möglichkeit, Apps (wie zum Beispiel Samsung Classroom Management, APPSFactory Clean-App, Antares EduCap) als APK auch im laufenden Betrieb auf die Geräte auszuspielen. Dies kann hilfreich sein, sofern eine Schülerin oder ein Schüler es doch schaffen sollte, Apps auf dem Gerät zu deinstallieren oder Geräte aus einer Reparatur neu ausgerollt werden. Definition: Applikationen sind alle Apps (-/-) Content. Content meint alle Files/Links/Movies/MP3s usw. die keine Apps sind. Erstere lassen sich über diesen Punkt steuern, Letztere über den Punkt “Inhalt” (siehe #08KM).	Aufgrund der experimentierfreudigen Natur der „Digital Natives“ sollte deshalb jedes mögliche Risiko für Manipulationen an Systemen minimiert werden, unabhängig davon, wie banal es erscheinen mag. Dieser Empfehlung kann dadurch Rechnung getragen werden, dass nur bestimmte Apps freigegeben werden.
#06 KM	Profil	Profile bieten die Möglichkeit, auf dem Gerät bestimmte Sicherheitseinstellungen zu	Letztere Maßnahme muss nur erfolgen, sofern hierzu überhaupt der Bedarf in der Schule besteht.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

		erzwingen (siehe hierzu die Empfehlungen zu KC, welche an dieser Stelle analog gelten). Bspw. die Kamera zu sperren/entsperren, Schnittstellen sperren/entsperren, Ortung deaktivieren, Wifi abschalten/erlauben etc. Eine Besonderheit von Knox Manage an dieser Stelle ist, dass hierüber die **VPN-Verbindung** in der Schule konfiguriert werden kann, was in Knox Configure nicht möglich ist. Weiter lassen sich App-Konfigurationen durchführen, was in KC ebenfalls nicht möglich ist. Beispielsweise besteht an dieser Stelle die Möglichkeit, E-Mail-Clients zu konfigurieren (also beim Exchange Server mit erlaubten Zugangsinformationen Anmeldungen vorzunehmen, oder eine gehashte Google-ID zu verwenden, die nicht schülerbezogen, sondern auf einen Google-Business Account bezogen ist).	Die Maßnahmen dienen ebenfalls der Gewährleistung der Systemintegrität gem. Art. 32 DSGVO. Insbesondere im BYOD-Case sind diese Maßnahmen empfehlenswert, soweit sinnvoll umsetzbar.
#07 KM	Kiosk	Über die Reiter “Kiosk” lässt sich der Startbildschirm, den die Schüler sehen, konfigurieren. Beispielsweise lässt sich einstellen, welche Links, PDFs und Apps auf dem Startbildschirm eingeblendet werden. Nach entsprechender Konfiguration können die Schüler ausschließlich mit diesen Inhalten arbeiten. Dies bietet die Möglichkeit, unnötige Datenverarbeitungen auszuschließen und die Geräte so zu konfigurieren, dass ausschließlich der Zweck der	Verarbeitung, Speicherung, Erfassung etc. von personenbezogenen Daten dürfen nicht unsystematisch erfolgen, sondern ausschließlich zweckgebunden, gem. Art. 5 Abs. 1 Buchst. b) DSGVO.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

		Verarbeitung erreicht werden kann.	
#08 KM	Inhalt	O.g. Inhalte (Inhalte meint alle Daten, die keine App sind, also Videos, Links, PDFs, MP3s etc.) können an dieser Stelle hochgeladen und anschließend über den Kiosk genutzt werden.	Diese Maßnahmen werden nur empfohlen, sofern sie die operativen Abläufe nicht störten. Sie dienen ebenfalls der Gewährleistung der Systemintegrität gem. Art. 32 DSGVO.
#09 KM	Verlauf	An dieser Stelle lässt sich einsehen, welcher Login-Name zu welchem Zeitpunkt welche Tätigkeit ausführte. Diese Dokumentation empfehlen wir, regelmäßig vom Systemadministrator im Beisein einer weiteren, neutralen Person einzusehen und abzulegen.	Durch die Dokumentation kann nachgewiesen werden, dass der Systemadministrator weiterhin für die Ausführung dieser Rolle geeignet ist.
#10 KM	Erweitert	Über die erweiterten Einstellungen lässt sich das System mit dem Active Directory der Schule verbinden. Beispielsweise lassen sich hierüber Schüler-Daten löschen, nachdem sie die Schule verlassen haben. Wir empfehlen einen Prozess einzuführen, damit dieser Schritt regelmäßig durchgeführt und dokumentiert wird.	Nach Artikel 17 Abs. 1 DSGVO sind personenbezogene Daten unverzüglich zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Dies ist im Falle eines Verlassens der Schule gegeben, sofern dem keine gesetzlichen Aufbewahrungsfristen entgegenstehen. Andernfalls ist Zweckfortfall aber spätestens nach Ablauf der gesetzlichen Aufbewahrungsfrist gegeben und spätestens zu diesem Zeitpunkt müssen die Daten gelöscht werden.

6.7. Antares / Edu-Pool

Hier haben die Lehrerin oder der Lehrer die Möglichkeit, den Edu-IDs Lerninhalte zuzuweisen, welche für die Schule oder den Schulträger von den Publishern (Schulbuch Verlagen) lizenziert wurden. Dabei gibt es systemseitig die Möglichkeit, dass ein Vermerk vorgenommen wird, welchem Schüler die Edu-ID zugewiesen wurde. Antares Project hat als “Datenschutz durch Technikgestaltung”-Maßnahme die maximale Zahl an möglichen Zeichen begrenzt, um zu verhindern, dass Lehrer hier den vollen Namen der Schüler eintragen. Unsere Empfehlung ist

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

es, Lehrer zusätzlich darauf zu verpflichten, an dieser Stelle maximal den Vornamen, besser noch einen Spitznamen zu hinterlegen, und die jeweilige Zuordnung separat zu vermerken.

Weiter hat Antares Mindestanforderungen für die Passwortsicherheit entsprechend der hier empfohlenen Passwortrichtlinie implementiert.

Lehrer erhalten die Möglichkeit, die Passwörter der Schüler zurückzusetzen, damit Letztere keine privaten E-Mail-Adressen hinterlegen müssen.

6.8. Verschlüsselung

Der Sicherheitscontainer verwendet eine 256-Bit-AES-Verschlüsselung. Nur bei korrekter Authentifizierung auf einem Samsung-Gerät werden die Daten entschlüsselt.

6.9. Löschkonzept

Die Edu-ID und die damit verknüpften personenbezogenen Daten werden zum Ende des Schuljahres automatisch gelöscht. Die Lehrer erhalten die Gelegenheit die Geräte nach Beendigung der Unterrichtsstunde zu bereinigen, für den Fall, dass die Geräte zur Benutzung durch andere Schüler in der Klasse verbleiben sollen. Hiervon soll nur in Ausnahmefällen (Nachprüfung) oder zur Einhaltung von landesspezifischen Aufbewahrungsfristen im Einzelfall abgewichen werden.

7. Nachwort

Bei den oben dargestellten Empfehlungen handelt es sich um eine Liste von Maßnahmen zur Einhaltung von datenschutzrechtlichen Pflichten, die wir mit bestem Wissen und Gewissen erstellt haben. An der Erstellung haben wir mit einem Team aus qualifizierten Juristen und IT-Fachkräften gearbeitet. Trotzdem lässt sich im Einzelfall nicht ausschließen, dass eine Landesbehörde in bestimmten Punkten einer abweichenden Rechtsaufassung folgen könnte. Dies soll nach unserem Dafürhalten jedoch kein Hindernis darstellen, da die an dieser Stelle beschriebenen Konfigurationsmöglichkeiten nicht abschließend sind und teilweise noch weitreichendere Beschränkungen möglich sind. Sollten Probleme auftreten, sollten diese mit dem zuständigen Datenschutzbeauftragten und dem Systemadministrator erörtert werden.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

8. Anlagen

8.1. VV-Muster für geplante Verarbeitungstätigkeiten

Samsung Neues Lernen

gem. Artikel 30 Abs. 1 DSGVO

Angaben zur datenverarbeitenden Stelle	
Name der Schule:	
Name der Schulleiterin oder des Schulleiters:	
Straße:	
Postleitzahl und Ort:	
Telefon:	
E-Mail-Adresse:	

Angaben zur Person der/des Datenschutzbeauftragten (Art. 37 ff. DSGVO)	
Anrede:	
Titel:	
Name:	
Dienstliche Anschrift	
Telefon:	
E-Mail-Adresse:	

Tätigkeit	Samsung Neues Lernen	
Zweckbestimmung	Integration digitaler Materialien in den Unterricht	
Rechtsgrundlage	[Bitte nach jeweiligem Landesrecht geltende Rechtsgrundlage einfügen.]	
Art der Verarbeitung	Erheben	
	Übermitteln	
Betroffene Person/en	Schülerinnen und Schüler	Lehrkräfte
Aufzählung der verarbeiteten personenbezogenen Daten	• Name • Edu-ID • Zugeteilte Lerninhalte,	• Name • Accountinformationen

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

(z.B. Namen oder Adressen)	Klassenzugehörigkeit • Geräteidentifikation (IMEI, MAC-Adresse, etc.) • Antworten auf Quizzes	• Zugeteilte Lerninhalte • Geräteidentifikation (IMEI, MAC-Adresse)

Tätigkeit	Samsung Neues Lernen	
Zweckbestimmung	Durchführung von Fernunterricht	
Rechtsgrundlage	[Bitte nach jeweiligem Landesrecht geltende Rechtsgrundlage einfügen.]	
Art der Verarbeitung	Erheben	
	Übermitteln	
Betroffene Person/en	Schülerinnen und Schüler	Lehrkräfte
Aufzählung der verarbeiteten personenbezogenen Daten *(z.B. Namen oder Adressen)*	• Wie vor • E-Mail-Adresse • Nutzungsdaten (Geräteinformationen, IP-Adresse, Videodaten) • Zugewiesene Unterrichtsstunden und -fächer • ausgetauschte Unterrichtsmaterialien und Dateien • Antworten auf Umfragen	• Wie vor • E-Mail-Adresse • Nutzungsdaten (Geräteinformationen, IP-Adresse, Videodaten) • Erstellte Unterrichtsstunden, und -fächer • Ausgegebene Unterrichtsmaterialien • Erstellte Umfragen

Zugriffsberechtigte	IT-Administration der Schule Schulleitung
Kategorien von Empfängern/ Datenübermittlung	**Intern:** Lehrer **Extern:** Auftragsverarbeiter Samsung und Antares Project GmbH [und ggf. Tabnova Inc. bei Nutzung für Fernunterricht] **Drittland:** Ja x Nein

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Liegt Auftragsverarbeitung vor?	x Ja Nein
Wenn ja, ist ein schriftlicher Vertrag zur Datenverarbeitung im Auftrag geschlossen?	x Ja Nein
Maßnahmen zur Erfüllung der Informationspflichten gegenüber den Betroffenen ***(Art. 13 DSGVO)***	Schriftlicher Hinweis zu Beginn des Schuljahres, Homepage Aushang Datenschutzerklärung, ausgespielt über Samsung Knox Configure auf die jeweiligen Endgeräte
Festgelegte Löschfristen	Die Edu-ID und alle damit verknüpften Informationen werden am Ende des jeweiligen Schuljahres automatisch gelöscht. Die personenbezogenen Daten werden im Übrigen unverzüglich gelöscht, sofern sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet werden, nicht mehr notwendig sind oder die zuvor erteilte Einwilligung widerrufen wurde. Dies ist in der Regel nach Ende der Unterrichtsstunde der Fall.
Datenschutzfolgenabschätzung	nicht erforderlich oder liegt vor/ Datum
Beschreibung getroffener technischer und organisatorischer Maßnahmen ***(Art. 32 Abs.1 DSGVO)***	**Analoge Verarbeitung:** • Aufbewahrung in einem abschließbaren Schrank, wenn ein Zugriff nicht erforderlich ist • Den Schlüssel für diesen Schrank haben nur die Zugriffsberechtigten **Digitale Verarbeitung:** • Sicherung der Rechner durch Passwort • Aufstellung der Rechner in verschließbaren Räumen • Rechte-/Rollenkonzept • Zentrale Vergabe der Zugriffsrechte durch den Administrator • Begrenzung der Zugriffsrechte auf die zuständigen Bediensteten

- Sicherung des Programmzugriffs durch einen Passwortschutz

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

8.2. Datenschutzerklärung zur Einfügung in Know Configure

(Schulbriefkopf ergänzen, gelb markierte Textteile anpassen)

Informationsblatt gemäß Art. 13 ff. Datenschutzgrundverordnung (DSGVO)
Sehr geehrte Eltern, sehr geehrte Erziehungsberechtigte, liebe Schülerinnen und Schüler,

hiermit informieren wir Sie bzw. dich über die Verarbeitung personenbezogener Daten in unserer Schule im Zuge der Verwendung der digitalen Lernangebote bei der Nutzung von Samsung Neues Lernen.

I. Datenverarbeitung
Die Schule erhebt und speichert personenbezogene Daten der Schülerinnen und Schüler zum Zwecke der **Erfüllung des Bildungsauftrags** oder der **Fürsorgeaufgaben**, zur **Erziehung** oder **Förderung** der Schüler oder zur Erforschung oder Entwicklung der **Schulqualität** oder **zur Erfüllung von Aufgaben der Schulaufsicht,** soweit dies erforderlich ist.

Rechtsgrundlage dieser Verarbeitung ist § [Hier Rechtsgrundlage für das jeweilige Bundesland einfügen].

Ohne eine rechtliche Grundlage ist die Verarbeitung personenbezogener Daten nur zulässig, wenn in die Verarbeitung eingewilligt wurde. Die betreffenden Daten können freiwillig von Ihnen bzw. dir angegeben worden sein.

II. Übermittlungen personenbezogener Daten

Im Rahmen unserer Teilnahme an Samsung Neues Lernen werden bestimmte Daten (die Edu-ID des jeweiligen Schülers, die Geräteidentifikationsdaten oder ggf. die während des Unterrichts zwischen den Endgeräten ausgetauschten Daten) an sogenannte Auftragsverarbeiter übermittelt, die unter Umständen ihrerseits Daten an ihre Unterauftragsverarbeiter offenbaren.

Antares verarbeitet auf Grundlage eines Vertrages als Auftragsverarbeiter weisungsgebunden personenbezogene Daten in unserem Auftrag zum Zwecke der

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Durchführung der digitalen Unterrichtseinheiten im Rahmen der Nutzung der Programme Classroom-Management App, EduPool und EduCap.

Die Samsung Electronics Co., Ltd. verarbeitet auf Grundlage eines Vertrages als Auftragsverarbeiter weisungsgebunden personenbezogene Daten in unserem Auftrag zum Zwecke der Bereitstellung der digitalen Infrastruktur (über Samsung Knox Configure, Knox Mobile Enrollment und Knox Manage gesteuerten Tablets und weiteren Endgeräte.

[ggf.: Bei der Nutzung der Classroom Management App zur Durchführung von Fernunterricht wird für die technische Abwicklung der Verbindung zwischen den Endgeräten eine Cloud-Infrastruktur benötigt. Zu diesem Zweck wurde ein Auftragsverarbeitungsvertrag mit dem Hersteller der App, Tabnova Inc. abgeschlossen, welche wiederum die Hetzner Online GmbH mit Sitz in Gunzenhausen mit dem Betrieb der Infrastruktur unterbeauftragt hat. Tabnova hat seinen Sitz in Großbritannien. Der Einsatz von Dienstleistern mit Sitz in Großbritannien ist durch einen sog. Angemessenheitsbeschluss der Europäischen Kommission rechtlich abgesichert.]

III. Dauer der Speicherung der personenbezogenen Daten

[Hier bitte konkrete Speicherdauer oder die Kriterien für ihre Festlegung einfügen, die für das Bundesland bzw. die jeweilige Schule gelten]

IV. Betroffenenrechte

Sie bzw. du können folgende Rechte geltend machen:

- **Auskunft/ Akteneinsicht**

Gem. Art. 15 DSGVO haben Sie bzw. hast du das Recht, Auskunft bzw. Akteneinsicht über die von uns verarbeiteten personenbezogenen Daten zu erhalten.

- **Berichtigung**

Sind bei uns gespeicherte personenbezogene Daten unrichtig oder unvollständig, haben Sie bzw. hast du gem. Art. 16 DSGVO das Recht, diese berichtigen bzw. vervollständigen zu lassen.

- **Löschung**

Art. 17 DSGVO normiert das Recht auf Löschung personenbezogener Daten. Dieses Recht steht Ihnen bzw. dir insbesondere dann zu, wenn die Speicherung der personenbezogenen Daten zur Erfüllung unserer gesetzlichen Aufgaben nicht mehr erforderlich ist oder du deine Einwilligung zur Datenverarbeitung mit Wirkung für die Zukunft widerrufen hast.

- **Einschränkung der Verarbeitung**

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Gem. Art. 18 DSGVO können Sie bzw. kannst du die Einschränkung der Verarbeitung der personenbezogenen Daten verlangen, wenn

- die Richtigkeit der Daten von dir bzw. Ihnen bestritten wird
- die Verarbeitung unrechtmäßig ist, Sie bzw. du aber deren Löschung ablehnen bzw. ablehnst
- wir die Daten nicht mehr benötigen, Sie bzw. du jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen
- oder Sie bzw. du gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung eingelegt hast.

- **Widerspruch**

Sie können bzw. du kannst bei Gründen, die sich aus Ihrer besonderen Situation ergeben, ein Widerspruchsrecht geltend machen. Gem. Art. 21 DSGVO ist jedoch zu berücksichtigten, ob schutzwürdige Gründe für die Verarbeitung vorliegen oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

- **Datenübertragbarkeit**

Ist die Verarbeitung Ihrer bzw. deiner Daten mit Hilfe eines automatisierten Verfahrens erfolgt, haben Sie bzw. hast du gem. Art. 20 DSGVO das Recht, die Daten in einem gängigen und maschinenlesbaren Format zu erhalten und an eine andere Schule zu übermitteln bzw. durch uns übermitteln zu lassen.

- **Widerruf der Einwilligung**

Sie haben bzw. du hast gem. Art. 7 Absatz 3 DSGVO das Recht, Ihre Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen.

- **Beschwerde**

Art. 77 DSGVO normiert ein Beschwerderecht bei der Aufsichtsbehörde. Die für uns zuständige Aufsichtsbehörde ist die Landesbeauftragte für den Datenschutz [Bundesland, Adresse, Kontaktdaten]

Eine Beschwerde kann über das auf der Homepage der Landesbeauftragten für den Datenschutz eingestellte Beschwerdeformular erfolgen.

V. Verantwortlicher und Datenschutzbeauftragter

Die datenverarbeitende Stelle ist die (Name der Schule, Anschrift).

Unseren Datenschutzbeauftragten erreichen Sie unter der E-Mail-Adresse (...).

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

8.3. Muster Datenschutzfolgenabschätzung (DSFA)

Nach Ansicht der Datenschutzkonferenz der Länder (DSK) ist vor dem Einsatz von Online-Lernplattformen vom Verantwortlichen (Schule oder Schulaufsichtsbehörde) eine Datenschutzfolgenabschätzung vorzunehmen, da nach Ansicht der DSK davon auszugehen ist, dass der Einsatz einer Lernplattform voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen zur Folge hat. Zwar handelt es sich bei **Samsung Neues Lernen** mit seinen Komponenten EduCAP, Classroom Manage und die Samsung KNOX Suite nicht um eine Lernplattform im herkömmlichen Sinne. Dennoch kann es zur Vermeidung rechtlicher Risiken empfehlenswert sein, eine Datenschutzfolgenabschätzung dennoch durchzuführen.

Um Ihnen diese schwierige Herausforderung zu erleichtern, stellen wir ein Muster zur Durchführung einer DSFA zur Verfügung. Es sei jedoch darauf hingewiesen, dass sich dieses Muster ausschließlich auf den Gegenstand dieses Datenschutzkonzeptes bezieht und nicht auf im Einzelfall zusätzlich genutzte Apps (wie bspw. Apps der Secuso Research Group, der Medienbildung Niedersachen, Neue Wege des Lernens e.V., des Landesmediumzentrums NRW etc.).

Mit der Folgenabschätzung sollen die spezifischen Risiken der automatisierten Verarbeitung personenbezogener Daten für die Rechte und Freiheiten der betroffenen Personen minimiert werden. Die gesetzliche Verpflichtung hierzu ergibt sich u. a. aus Art. 35 DSGVO:

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, 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, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Ziel dieser technisch-organisatorischen Analyse ist die Bewertung der Beherrschbarkeit neuer Informations- und Kommunikationsverfahren vor deren Einführung. Mit ihr werden die Abläufe der automatisierten Datenverarbeitung transparent gemacht, Gefahren für die

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Rechte der Betroffenen aufgezeigt, Risiken abgeschätzt und Sicherungskonzepte entworfen. Lassen sich erkannte Restrisiken nicht hinreichend sicher ausgestalten, darf ein Verfahren nicht zum produktiven Einsatz kommen. Stattdessen muss mit der zuständigen Datenschutzbehörde vorab konsultiert werden.

Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten ein. Das Ergebnis der Folgenabschätzung und seine Begründung sind schriftlich festzuhalten.

Grundlage für die Datenschutzfolgenabschätzung ist die Durchführung einer Risikobestimmung, die die Risiken, unter Berücksichtigung der existierenden TOMs (s.o.), für die Rechte und Freiheiten der betroffenen Personen ermittelt. Ergeben sich aus der Bestimmung Restrisiken sind die TOMs zu ergänzen, sodass die Eintrittswahrscheinlichkeit und/oder die Schadensschwere reduziert wird. Jeweils in einer Risikomatrix (siehe unten) sind einmal die Risiken vor Implementierung (Bruttorisiken) und einmal nach Implementierung TOM (Nettorisiken) auszuweisen.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Matrix zur Einstufung von Risiken (gem. BSI-Standard 200-3)

Wahrscheinlichkeit	Auswirkung/Schaden			
	Niedrig	Mittel	Hoch	Sehr hoch
Sehr wahrscheinlich (ca. einmal pro Woche oder öfter)	gering	mittel	hoch	**sehr hoch**
Wahrscheinlich (einmal pro Monat)	gering	mittel	hoch	hoch
Möglich (einmal pro Jahr)	gering	gering	mittel	mittel
Unwahrscheinlich (alle 10 Jahre oder seltener)	gering	gering	gering	gering

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

Muster-Struktur für einen Bericht über eine Datenschutz-Folgenabschätzung zur Einführung von Samsung Neues Lernen

Gemäß der Datenschutzgrundverordnung muss die Datenschutzfolgenabschätzung mindestens die folgenden Schritte enthalten:

(a) Beschreibung der Verarbeitungsvorgänge und Zwecke

Hierfür kann auf das Verzeichnis von Verarbeitungstätigkeiten zurückgegriffen werden. (s.o. unter VI. 1)

(b) Bewertung der Erforderlichkeit und Verhältnismäßigkeit der Verarbeitung im Verhältnis zum Zweck der Verarbeitung

Üblicherweise gelten hier die folgenden Erwägungen:

Eine sachgerechte Erfüllung des Bildungsauftrages und der gegenüber den Schülern bestehenden Fürsorgepflichten sowie eine Vorbereitung der Schüler auf das Leben im Zeitalter der Digitalisierung ist ohne den Einsatz von digitalen Lehrmethoden nicht möglich.

(c) Risikobewertung

Regelmäßig gelten hier die folgenden Erwägungen:
Der Einsatz der Lösung „Samsung Neues Lernen“ ist mit Risiken für die Sicherheit der personenbezogenen Daten der Betroffenen verbunden. Betroffen sind in erster Linie die Schüler. Ebenfalls betroffen sind Lehrkräfte, welche sich der Lösungen von Samsung Neues Lernen bedienen, um Ihre Schüler zu unterrichten. Die betroffenen Datenkategorien sind dem Verzeichnis von Verarbeitungstätigkeiten (s.o.) zu entnehmen.

Konkret besteht das Risiko, dass unbefugte Dritte (andere Schüler) Veränderungen an den in den Verarbeitungssystemen gespeicherten Daten vornehmen. Bei einer sachgerechten Konfiguration und Bedienung der Software besteht hierfür nur ein vernachlässigbares Risiko. Anders sieht es bei von den Nutzern gemachten Bedienungsfehlern und der unbefugten Weitergabe von Kennwörtern aus.

Unter Anwendung des Schutzstufenkonzepts der Landesbeauftragten für Datenschutz ist die Schutzstufe C betroffen, nur im unwahrscheinlichen Einzelfall (alle 10 Jahre oder seltener), ist eine Gefährdung von Daten, welche der Schutzstufe D unterliegen anzunehmen. Die unsachgemäße Handhabung der personenbezogenen Daten könnte die Betroffenen in dieser Ausnahmesituation in ihrer gesellschaftlichen Stellung

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

beeinträchtigen. Deutlich wird dies am Beispiel der einer Nichtversetzung von Schüler, aufgrund einer Veränderung von Daten im System.

Es besteht jedoch nur eine geringe Eintrittswahrscheinlichkeit, da hierfür zunächst (was nicht beabsichtigt wird) die Ergebnisse der Lernstände aus Samsung Neues Lernen zum Teil einer versetzungsrelevanten Benotung gemacht werden müsste und die betroffene Schülerin oder der betroffene Schüler zudem „auf der Kippe“ stehen müsste und es zusätzlich zu einer unbefugten Veränderung von Lernständen kommen müsste. Zudem sind die personenbezogenen Daten durch wirksame technische und organisatorische Maßnahmen vor dem unbefugten Zugriff durch Dritte geschützt.

(d) Technische und organisatorische Maßnahmen zur Bewältigung der Risiken

Der Einsatz von Samsung Neues Lernen wie auch von Samsung Knox erfordert das Vorliegen eines wirksamen Rechte-Rollenkonzept, das sicherstellt, dass auf darin gespeicherte personenbezogene Daten nur berechtigte Personen zugreifen können. In einem solchen Konzept sind folgende Festlegungen hinsichtlich Benutzergruppen zu treffen:

Administrator:	Lese- und Schreibzugriff auf sämtliche Daten, sowohl für Nutzerkonten als auch das Gesamtsystem Samsung Neues Lernen (Konfiguration Tabletts u. Installation der Apps).
Medienzentren:	Schreibzugriff auf die Accountvergabe für Schuladministratoren und Lehrkräfte
Schuladministratoren:	Schreibzugriff auf die Accountvergabe für Lehrkräfte.
Lehrkräfte:	Lese- und Schreibzugriff auf die Vergabe von Edu-IDs und die Zuweisung der lizenzierten Lerninhalte. Lesezugriff auf die Ergebnisse der Auswertungsbögen der Schüler.
Schüler	Lesezugriff auf die freigegebenen Lerninhalte. Lese- und Schreibzugriff auf Auswertungsbögen.

Der Zugriff auf die Systeme von “Samsung Neues Lernen” erfordert die Eingabe des Benutzernamens (im Falle der Lehrkräfte), bzw. der Edu-ID (im Falle der Schüler) und eines individuellen Passwortes. Das Passwort muss mindestens 8 Zeichen lang sein, Groß- und Kleinbuchstaben enthalten. Eines dieser Zeichen muss ein Sonderzeichen sein.

Die in den Systemen von Samsung Neues Lernen gespeicherten Daten sind durch eine 256-Bit-AES- Verschlüsselung gegen Zugriffe Unbefugter gesichert. Der Server, auf welchem die verschlüsselten Daten gespeichert sind, befindet sich im Falle von Samsung Knox bei

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl

AWS in Irland und unterliegt den folgenden Standards: SOC 1, SOC 2, SOC 3, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27001. Im Falle der von der Antares Project GmbH gespeicherten Daten, befindet sich der ebenfalls verschlüsselte und der Antares Project GmbH selbst gehörende Server in Deutschland. Bei den durch die Tabnova Inc. angemieteten Serverkapazitäten der Hetzner Online GmbH handelt es sich ebenfalls um ein ISO/IEC 27001 zertifiziertes Unternehmen.

[Hier Beschreibung der von Ihnen getroffenen Maßnahmen aus dem Punkt TOMs einfügen.]

Weitere Maßnahmen lassen sich dem Verzeichnis von Verarbeitungstätigkeiten entnehmen, sowie dem Datenschutzkonzept entnehmen.

(e) Ergebnis

Die Datenschutzfolgeabschätzung kommt zu dem Ergebnis, dass zwar ein Risiko der Schutzstufe C, bis in extremen Ausnahmefällen D, nach dem Schutzstufenkonzept der Landesbeauftragten für Datenschutz besteht, dieses jedoch durch die vorgesehenen technischen und organisatorischen Maßnahmen gut bewältigt werden kann. Da auch die Erforderlichkeit und Verhältnismäßigkeit der Verarbeitung im Verhältnis zum Zweck der Verarbeitung gegeben sind, bestehen nach Vornahme der Datenschutzfolgeabschätzung keine Bedenken gegen die Einführung der Samsung Neues Lernen Systeme.

Anmerkung: Die voranstehenden Ausführungen stellen eine musterhafte Beschreibung dar und geben lediglich eine grobe Struktur wider, nach der vorgegangen werden kann. Sie müssen von der verantwortlichen Schule oder Schulaufsichtsbehörde entweder selbst durchgeführt oder freigegeben werden. Ggf. sind noch besondere Vorgaben und Rechtsauffassungen der jeweiligen zuständigen Aufsichtsbehörden zu berücksichtigen.

secjur GmbH
Franz-Mayer-Str. 1
93053 Regensburg

Tel.: +49 941 569 550 20
E-Mail: dsb@secjur.com
Web: www.secjur.com

Amtsgericht Regensburg
HR-Nr.: HRB 17312
Steuer-Nr.: DE309721807

Sparkasse Regensburg
IBAN: DE81750500000027171347
BIC: BYLADEM1RBG

Geschäftsführung:
Niklas Hanitsch,
Manuel Stahl