Gutachten

zur datenschutzrechtlichen Zulässigkeit eines vollständig extern erfolgenden Hostings für „SWOP - Das Schul-Webportal“

(nachfolgend „Gutachten“ genannt)

für

SmartKomm GmbH
Rudolf-Breitscheid-Straße 42
14482 Potsdam

(nachfolgend „SmartKomm“ genannt)

erstellt durch

Rechtsanwalt Sascha Kremer
Stand: Freitag, 18. Mai 2018

Stand: 18. Mai 2018

1. Auftrag

SmartKomm bittet um eine rechtliche Begutachtung, ob und unter welchen Bedingungen der Betrieb des „SWOP - Das Schul-Webportal“ (im Folgenden „SWOP“) im Einklang mit datenschutzrechtlichen Bestimmungen vollständig auf externen Servern erfolgen kann, die nicht unter Kontrolle der Schule bzw. des Schulträgers stehen. Dabei sollen die externen Server nicht von SmartKomm selbst, sondern von einem für die SmartKomm tätigen Dienstleister (im Folgenden „Hosting-Provider“) als Subunternehmer betrieben werden.

Die Prüfung soll dabei unter besonderer Berücksichtigung der Datenschutz-Grundverordnung, des Bundesdatenschutzgesetzes in der neuen Fassung mit Wirkung vom 25.05.2018 sowie der Landesdatenschutzgesetze, Landesschulgesetze nebst - stellvertretend für andere - den zugehörigen Verordnungen der Länder Nordrhein-Westfalen und Hessen erfolgen. Eine Prüfung der einzelnen technischen Vorgänge, bei denen ein Umgang mit personenbezogenen Daten durch das SWOP erfolgt, ist nicht Gegenstand dieses Gutachtens.

Bei der rechtlichen Begutachtung wird vorausgesetzt, dass das Angebot des SWOP im Übrigen den datenschutzrechtlichen und schulrechtlichen Anforderungen entspricht. Dies betrifft insbesondere auch den Umgang mit Daten von Schülern, Eltern und Lehrern als solchen durch das SWOP.

2. Sachverhalt

SmartKomm bietet Schulen bzw. Schulträgern das SWOP an.
Bei SWOP handelt sich um ein interaktives Kommunikationssystem, das zum einen dem Informationsaustausch zwischen Schulleitung, Lehrern, Schülern und Eltern (im Folgenden zusammenfassend „Nutzer“) dienen und zum anderen die Schulleitung bei Schulverwaltungsangelegenheiten unterstützen soll. Dem einzelnen Nutzer werden dabei in geschützten Bereichen die Informationen zugänglich gemacht, für die er die entsprechenden Berechtigungen besitzt. Die Plattform dient damit im Wesentlichen dem Austausch schulischer Daten und Informationen; wegen der Einzelheiten wird auf die unter www.swop.schule.de zugänglichen Angaben Bezug genommen.

SWOP kann sowohl von öffentlichen Schulen als auch von Schulen in konfessioneller oder freier Trägerschaft genutzt werden.

Der Zugriff auf das SWOP erfolgt grundsätzlich browserbasiert. Dabei ist es technisch möglich, die Anwendung selbst entweder auf Servern im Hoheitsbereich der Schule zu speichern oder auf externen Servern. Aufgrund der damit verbundenen technischen und organisatorischen Anforderungen und Hardwarekosten bei einem Betrieb von SWOP auf schuleigenen Servern sind Schulen zunehmend daran interessiert, die Plattform von SmartKomm auf externen Servern betreiben zu lassen. Dabei ist eine Speicherung von Daten im SWOP ausschließlich auf solchen Servern vorgesehen, die innerhalb des EWR betrieben werden.

SmartKomm möchte für das vollständig außerhalb der Schule und Schulverwaltung erfolgende, also das externe Hosting des SWOP auf die Dienste von Hosting-Providern mit Sitz im EWR zurückgreifen. Dabei sollen alle Datenträger, auf denen sich Daten des SWOP befinden, verschlüsselt und vor einem Zugriff der Mitarbeiter des Hosting Providers physisch geschützt sein. Die Einrichtung und Administration des Servers sollen durch SmartKomm vorgenommen werden, Mitarbeiter des Hosting-Providers bekommen demnach zu keinem Zeitpunkt einen Zugang auf den Server.

3. Rechtliche Bewertung

3.1. Externe Datenspeicherung als datenschutzrechtlich relevanter Vorgang

Durch die Funktionen des SWOP werden Daten von Schülern, Eltern und Lehrern erhoben und in unterschiedlicher Weise verarbeitet und genutzt.
Inwieweit hierbei die Speicherung von Daten auf Servern eines Hosting-Providers datenschutzrechtlich zulässig ist, hängt entscheidend davon ab, ob eine solche Speicherung datenschutzrechtlich relevant ist. Nur dann greift das Regelungsregime des europäischen und deutschen Datenschutzrechts ein. Dies ist dann der Fall, wenn es sich bei den gespeicherten Daten um personenbezogene Daten gemäß Art. 4 Nr. 1 Datenschutz-Grundverordnung (im Folgenden „DS-GVO"), § 3 Abs. 1 Datenschutzgesetz Nordrhein-Westfalen (im Folgenden „DSG NW") oder § 2 Abs. 1 Hessisches Datenschutzgesetz (im Folgenden „HDSG") handelt.

3.1.1. Personenbezug bei einer Speicherung durch den Hosting-Provider

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann, vgl. Art. 4 Nr. 1 DS-GVO.

In diesem Sinne ist auch „Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder jedenfalls bestimmbarer natürlicher Personen" im Sinne der §§ 3 Abs. 1 DSG NW, 2 Abs. 1 HDSG zu verstehen. Ob eine Identifizierbarkeit vorliegt ist dabei abhängig davon, ob ein Dritter nach allgemeinem Ermessen die Identifizierung durchführen kann (vgl. ErwGr 26). Allgemeines Ermessen bedeutet, dass zwar nicht schlechterdings jede mögliche Identifizierbarkeit, jedenfalls aber die tatsächlich nicht gänzlich un- wahrscheinlichen (ungeachtet der Frage, ob sie legal sein mögen), in Betracht zu ziehen sind (vgl. Klabunde, in: Ehmann/Selmayr, DS-GVO Kommentar, 2017, Art. 4 Rn. 13; Ernst, in: Paal/Pauly, DS- GVO Kommentar, 2, Aufl. 2018, Art. 4 Rn. 8 ff.).

Insoweit ist jedenfalls beim Umgang mit Daten innerhalb des SWOP durch die hieran beteiligten Nutzer grundsätzlich von einem entsprechenden Personenbezug der Daten auszugehen. Die Funktionen des SWOP bieten Nutzern generell die Möglichkeit, ohne besonderen Aufwand die Identität anderer Nutzer des Systems zu bestimmen. Damit handelt es sich bei den im SWOP vorhandenen Daten aus Sicht aller Nutzer um personenbezogene Daten i.S.d. DS-GVO, des DSG NW und des HDSG.

Fraglich ist jedoch, ob die Daten im SWOP auch für den Hosting-Provider bestimmbar sind. Nach dem zu Grunde zu legenden Sachverhalt (siehe oben Ziff. 2) sollen technische und organisatorische Maßnahmen im Sinne einer Verschlüsselung der gespeicherten Daten und eines physischen Zugriffschutzes eine Kenntnisnahme der Daten durch Mitarbeiter des Hosting-Providers verhindern.

Teilweise wird bei einer solchen technischen und organisatorischen Zugriffssicherung die Auffassung vertreten, dass eine Kenntnisnahme der Daten durch den Hosting-Provider und damit die Möglichkeit der Zuordnung zu bestimmten Personen mit einem unverhältnismäßig hohen Aufwand verbunden wäre. Dies hätte zur Folge, dass eine Speicherung der Daten beim Hosting-Provider grundsätzlich nicht in den Anwendungsbereich des Datenschutzrechts fallen würde (Heidrich/Wegener, MMR 2010, 803 [806], noch zum BDSG a.F.).

Dabei ist jedoch zu berücksichtigen, dass die Sicherheit entsprechender technischer und organisatorischer Maßnahmen generell nicht mit letzter Gewissheit beurteilt werden kann. Aufgrund stetig wachsender technischer Möglichkeiten können etwa heute als sicher eingestufte Verschlüsselungsmethoden unsicher werden; ebenso könnten Schlüssel zur Entschlüsselung in die Hände unbefugter Dritter fallen (vgl. Dammann, in: Simitis, BDSG Kommentar, 7. Auflage 2011, § 3 Rn. 38; Beck'scher Online-Kommentar, Stand: 1.8.2012, § 3 BDSG Rn. 107; siehe zum Diskussionsstand auch Spies, MMR-Aktuell 2011, 313727). Solche technologischen Entwicklungen sind bei der Beurteilung nach der Rechtslage unter der DS-GVO zu berücksichtigen (ErwGr 26).

Jedenfalls dann, wenn die Verschlüsselung gebrochen wird, ist ohne weiteres von einer Bestimmbarkeit der jeweils betroffenen Nutzer auszugehen, sodass spätestens ab diesem Zeitpunkt von einem Personenbezug und der Anwendbarkeit datenschutzrechtlicher Vorschriften auszugehen ist. Ist die Speicherung dann nicht datenschutzrechtlich legitimiert, ist sie rechtswidrig. Der Umstand, dass ein Personenbezug ex ante mit verhältnismäßigen Mitteln nicht herstellbar erschien, befreit insoweit nicht von der datenschutzrechtlichen Haftung, wenn dieser Fall dennoch eintritt (vgl. Klabunde, in: Eh- mann/Selmayr, DS-GVO Kommentar, 2017, Art. 4 Rn. 13; Ernst, in: Paal/Pauly, DS-GVO Kommentar, 2, Aufl. 2018, Art. 4 Rn. 8 ff.).

Es ist daher angesichts der insoweit unsicheren Sach- und Rechtslage aus Gründen der Risikovorsorge dringend zu empfehlen, auch die beim Hosting-Provider im Rahmen des SWOP gespeicherten Daten der betroffenen Personen höchstvorsorglich als personenbezogene Daten zu behandeln (so schon zum BDSG a.F. auch Dammann, in: Simitis, a.a.O., § 3 BDSG Rn. 38; Art. 29 Datenschutzgruppe, WP 136 Abschnitt III 3, Seite 19). Im Folgenden wird daher davon ausgegangen, dass auch auf die beim Hosting-Provider gespeicherten Daten den rechtlichen Vorgaben des Datenschutzes unterliegen.

3.1.2. Notwendigkeit der datenschutzrechtlichen Legitimation der Speicherung

Grundsätzlich stellt jede Speicherung personenbezogener Daten einen datenschutzrelevanten Vor- gang dar, vgl. Art. 4 Nr. 2 DS-GVO, § 3 Abs. 2 Nr. 2 DSG NW, § 2 Abs. 2 Nr. 2 HDSG. Als solche ist die Speicherung nur dann und soweit zulässig, als eine Rechtsvorschrift dies erlaubt oder der Betroffenen zuvor sein Einverständnis mit der Verarbeitung erklärt hat, vgl. Art. 6 Abs. 1 DS-GVO, § 4 Abs. 1 DSG NW, § 7 Abs. 1 HDSG. Die rechtliche Verantwortung für eine datenschutzkonforme Speicherung der Daten beim Hosting-Provider trägt dabei gegenüber den

betroffenen Personen der nach dem einschlägigen Datenschutzgesetz „Verantwortliche“ bzw. die „verantwortliche Stelle“. „Verantwortlicher“ ist dabei im Wesentlichen „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“, vgl. Art. 4 Nr. 7 DS-GVO. In diesem Sinne ist auch die „verantwortliche Stelle“, „die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“ auszulegen, vgl. §§ 3 Abs. 3 DSG NW, 2 Abs. 3 HDSG.

3.2. Verantwortlicher für die Einhaltung datenschutzrechtlicher Vorschriften

Angesichts der unterschiedlichen Funktionalitäten des SWOP kommen als Verantwortlicher sowohl SmartKomm selbst als auch die Schule als jeweiliger Vertragspartner von SmartKomm in Betracht. Je nachdem, wer jeweils in welchem Zusammenhang als Verantwortlicher zu identifizieren ist, können dabei die Möglichkeiten einer datenschutzrechtlichen Legitimation der Speicherung der Daten der betroffenen Personen beim Host-Provider gegebenenfalls unterschiedlich zu bewerten sein.

3.2.1. SmartKomm als Verantwortlicher

Eine wichtige Funktionalität des SWOP besteht in der Möglichkeit von Schülern, Eltern und Lehrern, Informationen auf die Plattform einzustellen, zu editieren und mit anderen zu teilen. SWOP weist insoweit die klassischen Merkmale eines Sozialen Netzwerks auf.

Indem die Schule bzw. der Schulträger mit SmartKomm einen Vertrag über die Nutzung des SWOP abschließt, eröffnen sie Schülern, Eltern und Lehrern die Möglichkeit, SWOP in entsprechen- der Weise zu nutzen. Nach dem zu Grunde zu legenden Sachverhalt (siehe oben Ziff. 2) greift die Schule selbst allerdings in den Umfang und die Art der Nutzung des SWOP als Sozialem Netzwerk grundsätzlich nicht ein. Vielmehr beschränkt sich die Rolle der Schule diesbezüglich im Wesentlichen auf die Bereitstellung eines Zugangs zum SWOP.

Es lässt sich daher mit guten Argumenten die Auffassung vertreten, dass die Schule hinsichtlich dieser Funktion des SWOP nicht Verantwortlicher im Sinne der Datenschutzgesetze ist. Vielmehr kommt bei der erstmaligen Nutzung des SWOP durch den jeweiligen Schüler, die Eltern sowie Lehrer zwischen diesen und SmartKomm ein unmittelbares Nutzungsverhältnis zustande. Dies gilt unabhängig davon, dass die Schule bzw. der Schulträger mit SmartKomm den (zivilrechtlichen) Lizenzvertrag über die Nutzung des SWOP schließt.

Das Soziale Netzwerk als Telemediendienst im Sinne von § 1 Telemediengesetz (im Folgenden „TMG“) wird unmittelbar von SmartKomm gegen- über den Nutzern erbracht. SmartKomm, nicht die Schule, gibt den Nutzern maßgeblich die Funktionalitäten und Nutzungsmöglichkeiten des SWOP als Sozialem Netzwerk vor und entscheidet damit eigenständig über die damit verbundenen Verwendungsmöglichkeiten der durch das SWOP als sozialem Netzwerk verarbeiteten personenbezogenen Daten.

Hiernach ist davon auszugehen, dass eine Speicherung personenbezogener Daten der betroffenen Nutzer auf Servern des Hosting-Providers im Rahmen der Funktionalitäten des SWOP als Sozialem Netzwerk in erster Linie zur Erbringung des Telemediendienstes durch SmartKomm

gegenüber den Nutzern erfolgt. In diesem Fall ist dann SmartKomm aber auch verantwortliche Stelle für eine datenschutzrechtlich zulässige Datenspeicherung.

Etwas anderes könnte nur dann gelten, wenn die Schule bzw. der Schulträger maßgeblichen Einfluss auf den Zugriff auf die im Rahmen der Funktion als Sozialem Netzwerk im SWOP genutzten Daten der Betroffenen hätte, etwa das SWOP weitreichend individuell auf die Wünsche und Bedürfnisse der Schule bzw. des Schulträgers angepasst würden. Dies ist nach dem zu Grunde zu legenden Sachverhalt allerdings nicht der Fall.

3.2.2. Schule als Verantwortlicher

Die Funktionalitäten des SWOP gehen über das Angebot eines Sozialen Netzwerks durch SmartKomm als Diensteanbieter hinaus. So bietet das SWOP der Schulleitung die Möglichkeit, Informationen zum Lernverhalten von Schülern zur Vorbereitung von Elterngesprächen einzusehen, Dokumentenbibliotheken für Lehrer anzulegen, diesen in geschützten Bereichen Nachrichten zu hinter- lassen, Kalenderfunktionalitäten zu nutzen oder Noten der Schüler zentral abzulegen.

Damit nutzen nicht nur Schüler, Eltern und Lehrer den von SmartKomm betriebenen Telemediendienst, sondern auch die Schulverwaltung selbst zu eigenen Zwecken. Hierzu stellt die Schulverwaltung auch Daten von Schülern, Eltern und Lehrern in das System ein. Auf Grundlage des zwischen der Schule bzw. der Schulverwaltung und SmartKomm bestehenden Lizenzvertrags über SWOP fungiert SmartKomm gegenüber der Schulverwaltung als ihrem Vertragspartner insoweit als IT- Dienstleister. SmartKomm stellt die Plattform bereit, damit die Schulverwaltung diese für ihre eigenen Zwecke nutzen kann.

Kommt es in diesem Zusammenhang dann aber zu einer Speicherung personenbezogener Daten von Eltern, Schülern oder Lehrern auf den Servern des Hosting-Providers ist davon auszugehen, dass hierfür die Schule selbst die datenschutzrechtliche Verantwortung trägt.

3.2.3. Zwischenergebnis

Es ist festzuhalten, dass – abhängig von den konkreten Funktionalitäten des SWOP – sowohl SmartKomm selbst als auch die Schule als Verantwortlicher im Sinne der Datenschutzgesetze die Verantwortung für die datenschutzrechtliche Zulässigkeit einer Speicherung der Daten von Schülern, Eltern und Lehrer bei einem externen Hosting-Provider tragen.

3.3. Zulässigkeit der Datenspeicherung beim Hosting-Provider

Für die Frage der Zulässigkeit der Datenspeicherung auf einem Server des externen Hosting-Providers ist im Folgenden zwischen der Verantwortlichkeit von SmartKomm und der Verantwortlichkeit der Schule für die Speicherung zu differenzieren.

3.3.1. SmartKomm als Verantwortlicher und Zulässigkeit der Speicherung

Soweit SmartKomm im Hinblick auf die Funktionen des SWOP als Sozialem Netzwerk verantwortliche Stelle ist, ist SmartKomm grundsätzlich in den Grenzen von Art. 6 DS-GVO auch zur Speiche- rung der Daten der Betroffenen berechtigt, d.h. soweit dies zur Erbringung des Telemediendienstes und damit des SWOP erforderlich ist.

Bei einer Auslagerung des SWOP auf einen Hosting-Provider findet die Speicherung jedoch nicht bei SmartKomm selbst, sondern bei einem Dritten statt. Hierfür ist eine eigene datenschutzrechtliche Legitimation erforderlich, die eine solche Datenspeicherung außerhalb des unmittelbaren Herrschaftsbereichs von SmartKomm zulässt. Dabei finden auf SmartKomm als nicht-öffentliche Stelle, d.h. Privatunternehmen, grundsätzlich die Vorschriften der DS-GVO Anwendung, vgl. Art. 2 DS-GVO.

3.3.1.1. Einwilligung als Legitimation der Speicherung beim Hosting-Provider

Eine solche Speicherung beim Hosting-Provider ist grundsätzlich dann zulässig, wenn jeder hiervon betroffene Nutzer vor der erstmaligen Speicherung jeweils formwirksam in die Weitergabe der Da- ten an den Hosting-Provider und die Speicherung auf seinen Servern einwilligt, Art. 6 Abs. 1 lit. a), Art. 7 DS-GVO. Dabei ist unter anderem erforderlich, dass die Einwilligung eindeutig und freiwillig erklärt wird, etwa durch das Ankreuzen eines entsprechenden Kästchens in einem Online-Formular, Umfang und Zweck der Speicherung der betroffenen Person vor ihrer Einwilligung transparent dargestellt, die Einwilligung protokolliert wird und die Einwilligung von der betroffenen Person je- derzeit abrufbar sowie jederzeit mit Wirkung für die Zukunft widerrufbar ist. Soweit Schüler betroffen sind, die das 16. Lebensjahr noch nicht vollendet haben (in der Sprache der DS-GVO „Kinder“), ist die Einwilligung durch den Träger der elterlichen Sorge zu erklären, Art. 8 Abs. 1 DS-GVO.

Generell wären daher die mit einer Einwilligungslösung verbunden Rahmenbedingungen für Smart- Komm mit einem erheblichen technischen und organisatorischen Aufwand verbunden. Dabei ist insbesondere zu beachten, dass bei Widerruf der Einwilligung durch eine betroffene Person eine weitere Speicherung ihrer Daten beim Hosting-Provider unzulässig wäre, so dass bei jedem Wider- ruf eine Löschung der Daten der betroffenen Person auf Servern des Hosting-Providers sichergestellt werden müsste. Dies würde es u.U. erforderlich machen, neben der Server-Infrastruktur beim Hosting-Provider eine zweite, alternative Infrastruktur bei SmartKomm selbst für den Fall vorzusehen, dass eine Einwilligung eines Nutzers zur Datenauslagerung nicht erteilt oder später widerrufen wird.

Aufgrund der hohen technischen und organisatorischen Anforderungen an ein rechtskonformes Einwilligungsmanagement sollte eine Einwilligungslösung zur Legitimierung der Datenspeicherung beim Hosting-Provider daher nur dann ernsthaft in Betracht gezogen werden, falls alternativ hierzu keine anderweitige gesetzliche Legitimationsmöglichkeit in Betracht kommt (vgl. hierzu nachfolgend Ziff. 3.3.1.2).

3.3.1.2 Auftragsverarbeitung zur Legitimation beim Hosting-Provider

Auch ohne Einwilligung der Betroffenen wäre eine Datenspeicherung durch den Hosting-Provider im Rahmen der Nutzung des SWOP als Sozialem Netzwerk auf Servern innerhalb des EWR dann datenschutzrechtlich zulässig, wenn

- die Speicherung durch den Hosting-Provider im Auftrag der SmartKomm erfolgt und

- die gesetzlichen Anforderungen der Art. 28 f., 32 DS-GVO an die Auftragsverarbeitung eingehalten werden.

In diesem Fall wäre der Hosting-Provider nicht „Dritter" im Sinne des Art. 4 Nr. 10 DS-GVO, sondern lediglich Empfänger im Sinne des Art. 4 Nr. 9 DS-GVO, datenschutzrechtlich also den Weisungen der SmartKomm unterworfen, die damit allein Verantwortlicher wäre.

3.3.1.2.1. Hosting-Provider als Auftragsverarbeiter

Eine Auftragsverarbeitung ist dadurch charakterisiert, dass sich der Auftraggeber eines (nicht im Sinne der DS-GVO) Dritten als Auftragnehmer bedient, der lediglich weisungsgebunden mit den Daten umgeht. Der Auftragnehmer fungiert dabei als „verlängerter Arm" oder als ausgelagerte Abteilung des Auftraggebers. Dieser bleibt „Verantwortlicher" und behält als „Herr der Daten" die volle Entscheidungsbefugnis über den Datenumgang, so dass der Auftragnehmer keinerlei inhaltlichen Bewertungs- und Ermessensspielraum über die Erhebung, Verarbeitung oder Nutzung hat (Martini, in: Paal/Pauly, a.a.O., Art. 28 Rn. 28 ff.; vgl. auch Gola/Schomerus, a.a.O., § 11 Rn. 3; Petri, in Simitis, a.a.O., § 11 Rn. 20).

Nach dem zu Grunde zu legenden Sachverhalt stellt der Hosting-Provider auf seinen Servern ausschließlich Platz zur Speicherung von Daten des SWOP zur Verfügung. Irgendwelche Kompetenzen zum weiteren Datenumgang werden dem Hosting-Provider nicht eingeräumt. Er leistet damit SmartKomm lediglich eine technische Hilfestellung, ist selbst an den Daten aber nicht interessiert. Die Inanspruchnahme von Speicherplatz bei einem Hosting-Provider ist daher eine typische Maßnahme der Auftragsverarbeitung (Bertermann, in: Ehmann/Selmayr, a.a.O., Art. 30 Rn. 11; insoweit übertragbar: Taeger/Gabel, BDSG Kommentar, 2010, § 11 Rn. 18; Redeker, IT-Recht, 12. Auflage 2012, Rn. 953).

Der Auftragscharakter wird dabei nicht dadurch ausgeschlossen, dass der Auftragnehmer, d.h. der Hosting-Provider, durch die Speicherung der Daten auch seinen vertraglichen Verpflichtungen mit SmartKomm nachkommt und daher auch ein Eigeninteresse an der Speicherung hat (Gola/Schomerus, a.a.O., § 11 Rn. 7a). Im Vordergrund und damit entscheidend für die rechtliche Einordnung ist die Weisungsgebundenheit des Hosting-Providers und damit der Auftragscharakter der Dienstleistung.

Wird der Hosting-Provider gegenüber SmartKomm als Auftragnehmer einer Auftragsverarbeitung tätig, ist die Datenspeicherung auf seinen Servern grundsätzlich zulässig, wenn die Auftragsverarbeitung den Anforderungen von Art. 28 f., 32 DS-GVO entspricht.

3.3.1.2.2. Prüfung der Maßnahmen zur Datensicherheit

Nach Art. 28 Abs. 1 DS-GVO ist der Hosting-Provider von SmartKomm unter besonderer Berücksichtigung seiner Eignung, die hinreichend Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet, sorgfältig auszuwählen.

Da SmartKomm nach Art. 28 Abs. 3 S. 1, 2 lit. a DS-GVO einen Auftragsverarbeitungsvertrag mit dem Hosting-Provider abzuschließen hat, der auch die Ergreifung der nach Art. 32 DS-GVO erforderlichen Maßnahmen durch den Auftragsverarbeiter vorsieht , ist SmartKomm dringend zu empfehlen, sich vor Vertragsabschluss mit einem Hosting-Provider von diesem ein Konzept der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO (im Folgenden „Datensicherheitskonzept“) vorlegen zu lassen und dieses auf seine Angemessenheit zu überprüfen. Dabei sollte sich das Datensicherheitskonzept zwar grundsätzlich an den datensicherheitsrechtlichen Anforderungen nach Art. 32 DS-GVO orientieren. Es darf sich aber nicht in der bloßen Wiedergabe des Gesetzestextes erschöpfen, sondern muss die konkret getroffenen Maßnahmen benennen, die geeignet sind, die Sicherheit der im SWOP gespeicherten, (u.U. auch besonderen Kategorien von) personenbezogen Daten der Nutzer zu gewährleisten.

Eine Vor-Ort-Überprüfung, ob die vom Hosting-Provider angegebenen Datensicherheitsmaßnahmen auch tatsächlich eingehalten werden ist zwar grundsätzlich empfehlenswert, aber nicht zwingend geboten, sofern SmartKomm auch anderweitig sicherstellen kann, dass der Hosting-Provider die Garantien im Sinne des Art. 28 Abs. 1 bietet (insoweit übertragbar: Petri, in: Simitis, a.a.O., § 11 Rn. 59; Gola/Schomerus, a.a.O., § 11 Rn. 21). Dies kann etwa durch Einschaltung von sachverständigen Dritten, durch Fragebögen oder durch die Anforderung von Prüfergebnissen oder Zertifikaten beim Hosting-Provider erfolgen (Gola/ Schomerus, a.a.O., § 11 Rn. 21). Ein Kontrollrecht und die korrespondierende Duldungs- und Mitwirkungspflicht wird SmartKomm jedoch schon wegen Art. 28 Abs. 3 S. 2 lit. h DS-GVO vertraglich vereinbaren müssen.

3.3.1.2.3. Dokumentationspflicht

Die Ergebnisse der Prüfungen des Hosting-Providers durch SmartKomm sollte dokumentiert werden. Diese Dokumentation sollte beweissicher und daher im Regelfall in Papierform erfolgen, weil ansonsten im Zweifel insbesondere der Nachweis gegenüber der Aufsichtsbehörde, dass SmartKomm auf die Einhaltung der Garantien nach Art. 28 Abs. 1 DS-GVO hingewirkt hat, kaum zu führen sein wird. Überdies sind gemäß Art. 28 Abs. 3 S. 2 lit. a DS-GVO die Weisungen an den Auftragneh- mer zu dokumentieren. Hierfür bietet sich das Verzeichnis über die Verarbeitungstätigkeiten nach Art. 30 DS-GVO an.

3.3.1.2.4. Schriftliche Vereinbarung zur Auftragsverarbeitung

Gemäß Art. 28 Abs. 3 S. 1, Abs. 9 DS-GVO ist der Auftragsverarbeitungsvertrag schriftlich zu erteilen, wobei auch ein elektronisches Format dem Formerfordernis genügt. Die zwischen SmartKomm und dem Hosting-Provider zu treffende Vereinbarung muss dabei insbesondere

Einzelheiten zu den in Art. 28 Abs. 3 S. 2 DS-GVO aufgeführten Punkten enthalten. Dabei haben die Parteien allerdings hinsichtlich des „Wie“ der vertraglichen Ausgestaltung einen weiten Ermessensspielraum. Ein ge- eigneter Vertragstext wird der SmartKomm im Anschluss an diese Stellungnahme zur Verfügung gestellt.

3.3.2. Schule als Verantwortlicher und Zulässigkeit der Speicherung

Soweit die Schule Verantwortlicher für den Datenumgang ist und sich selbst des SWOP bedient, erfolgen die diesbezüglichen Verarbeitungen primär zu Zwecken der Schulverwaltung. SmartKomm als IT-Dienstleister wird insoweit durch die Bereitstellung der Plattform für die Schule sowie Wartungs- und Pflegeleistungen unterstützend tätig, hat jedoch kein weitergehendes eigenes Interesse an den Daten. Insbesondere besitzt SmartKomm keine selbständige Befugnis zur Bearbeitung, Löschung oder anderweitigen Verarbeitung der Daten.

SmartKomm ist daher im Rahmen einer entsprechenden Nutzung des SWOP durch die Schule – vergleichbar einem Cloud-Provider oder Application Service Provider (vgl. Redeker, a.a.O., Rn. 1128; Ehmann, in: Simitis, a.a.O., § 10 Rn. 21) – als Auftragnehmer einer datenschutzrechtlichen Auftragsverarbeitung durch die Schule als Auftraggeber zu qualifizieren. Der Hosting-Provider wird in diesem Fall als Subunternehmer (gleichsam „weiterer Auftragsverarbeiter“ im Sinne des Art. 28 Abs. 2, 4 DS-GVO) von SmartKomm zur Erfüllung von deren Verpflichtungen gegenüber der jeweiligen Schule tätig.

Ob und unter welchen rechtlichen Voraussetzungen eine solche Auslagerungskonstruktion datenschutzrechtlich zulässig ist, hängt dabei davon ab, in welcher Trägerschaft die Schule jeweils geführt wird, da dies Einfluss auf die anzuwendenden datenschutzrechtlichen Vorschriften hat.

3.3.2.1. Schulen in öffentlicher Trägerschaft in Nordrhein-Westfalen

Soweit es sich um öffentliche Schulen in Nordrhein-Westfalen handelt finden auf sie die Vorschriften des DSG NW sowie die datenschutzrechtlichen Regelungen des Schulgesetzes und der hierzu erlassenen datenschutzrechtlichen Verordnungen Anwendung. Dabei gehen die speziellen Vorschriften des Schuldatenschutzes den allgemeinen landesdatenschutzrechtlichen Regelungen grundsätzlich vor.

3.3.2.1.1. Datenschutzrechtliche Anforderungen an die externe Speicherung von Schuldaten

Den speziellen Vorschriften der §§ 120 bis 122 Schulgesetz NRW ist kein generelles Verbot der externen Speicherung personenbezogener Daten von Schülern, Eltern und Lehrern im Wege der Auftragsverarbeitung zu entnehmen. Die Vorschriften enthalten die grundlegenden Bestimmungen für die Verarbeitung personenbezogener Daten von Schülern, Eltern und Lehrern im Bereich öffentlicher Schulen in Nordrhein-Westfalen.

Zu beachten ist jedoch, dass vom Verordnungsgeber zur näheren Ausgestaltung des nordrhein-westfälischen Schuldatenschutzes auf Grundlage von § 122 Abs. 4 Schulgesetz NRW die „Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (im Folgenden „VO-DV I“) sowie die Verordnung über die zur Verarbeitung zugelassenen Daten der Lehre- rinnen und Lehrer (im Folgenden „VO-DV II“) erlassen wurden. § 2 Abs. 1 der jeweiligen Verordnung sieht dabei vor, dass die automatisierte Verarbeitung der

personenbezogenen Daten ausschließlich auf solchen Arbeitsplätzen zulässig ist, die für Verwaltungszwecke eingerichtet sind. Dies schließt eine Auftragsverarbeitung und damit auch die Auslagerung der Speicherung von Daten von Schülern, Eltern oder Lehrern indes nicht aus.
In § 2 Abs. 3 VO-DV I bzw. § 3 VO-DV II heißt es dazu:

> „Die Schulen und Schulaufsichtsbehörden sind berechtigt, unter Beachtung der Voraussetzung des § 11 DSG NRW die Datensicherheit gewährleistende und zuverlässige Institutionen mit der Verarbeitung ihrer Daten zu beauftragen. Die Datenverarbeitung im Auftrag ist nur zulässig nach Wei- sung der Schule oder der Schulaufsichtsbehörden und ausschließlich für deren Zwecke."

Den allgemeinen Vorschriften des DSG NW sind keine Regelungen zu entnehmen, die über diese speziellen Regelungen hinaus eine Speicherung bei einem Hosting-Provider datenschutzrechtlich untersagen oder beschränken würde. Insgesamt ist damit festzuhalten, dass eine externe Speicherung von Daten beim Hosting-Provider im Wege der Auftragsverarbeitung zulässig ist, wenn diese unter den Bedingungen der §§ 2 Abs. 3 VO-DV I, 3 VO-DV II, 11 DSG NW erfolgt.

Dabei weisen die gesetzlichen Anforderungen des § 11 DSG NW nicht den gleichen Detailierungsgrad wie die Vorschriften der Art. 28 f., 32 DS-GVO auf, gehen allerdings auch nicht über diese hin- aus. Aufgrund der relativ detaillierten und weitgehenden Anforderungen der DS-GVO, insbesondere im Hinblick auf die zu treffenden Maßnahmen zur Datensicherheit und im Sinne einer möglichst weitgehenden Standardisierung etwaiger Mustervertragsdokumente zur Verwendung in verschiedenen Bundesländern empfiehlt sich daher, sich bei der Erstellung eines Vertragsmusters zur Auftragsverarbeitung grundsätzlich an den Vorgaben der DS-GVO zu orientieren.

3.3.2.1.2. Parteien der Auftragsverarbeitung

Zu berücksichtigen ist, dass die erforderliche Vereinbarung zur Auftragsverarbeitung nicht zwischen der Schule und dem Hosting-Provider, sondern zwischen der Schule und SmartKomm als Anbieter der Plattform zu schließen wäre. SmartKomm würde wiederum einen Vertrag mit dem Hosting-Provider schließen, der dabei als Subunternehmer die Datenspeicherung für SmartKomm übernimmt.

Um die gegenüber der Schule im Rahmen der Vereinbarung zur Auftragsverarbeitung zuzusichern- den Maßnahmen zur Datensicherheit bei der Datenspeicherung auch erfüllen zu können, ist Smart- Komm daher zu empfehlen, sich zunächst die technisch-organisatorischen Maßnahmen von dem Hosting-Provider vorlegen zu lassen. Diese sollten dann der Schule zu deren Kontrolle vorgelegt und zum Bestandteil der Vereinbarung zur Auftragsverarbeitung mit der Schule gemacht werden.

Ein solches Vorgehen sollten SmartKomm grundsätzlich ohne weiteres unproblematisch möglich sein, da sie selbst aufgrund der vorstehenden Erwägungen (siehe oben Ziff. 3.3.1.2) diesbezügliche Informationen zum Abschluss ihrer Vereinbarung zur Auftragsverarbeitung mit dem Hosting-Provider benötigt.

Im Rahmen der Vereinbarung zur Auftragsverarbeitung sollte SmartKomm dabei darauf achten, dass in der Vereinbarung zur Auftragsverarbeitung mit der jeweiligen Schule auch das Recht zur

Beauftragung des Hosting-Providers als Subunternehmer vorgesehen wird. Im Regelfall verpflichtet sich SmartKomm im Gegenzug dazu, die zwischen ihr und der Schule getroffenen Vereinbarungen auch dem Hosting-Provider aufzuerlegen. Eine Übertragung von Verpflichtungen aus dem Vertragsverhältnis zwischen der Schule und SmartKomm auf das Vertragsverhältnis zwischen SmartKomm und dem Hosting-Provider empfiehlt sich für SmartKomm aber auch deswegen, weil so SmartKomm gegebenenfalls Rückgriff beim Hosting-Provider nehmen kann, wenn SmartKomm aufgrund eines Fehlverhaltens des Hosting-Providers seine vertraglichen Verpflichtungen gegenüber der Schule verletzen sollte.

Um die Komplexität und Anzahl der unterschiedlichen Vertragsdokumente möglichst gering zu halten empfiehlt es sich dabei für SmartKomm, die Regelungen zur Auftragsverarbeitung zwischen SmartKomm und dem Hosting-Provider im Zusammenhang mit der Funktion von SWOP als Sozialem Netzwerk möglichst identisch mit den Regelungen im Rahmen einer Subunternehmervereinbarung mit dem Hosting-Provider bei Nutzung des SWOP der Schule zur Schulverwaltungszwecken auszugestalten. Es könnte dann lediglich ein Vertrag mit dem externen Hosting-Provider geschlossen werden, der beide Regelungsbereiche zugleich abdeckt. Auch insoweit wird der Smart- Komm im Anschluss an diese Stellungnahme ein geeigneter Vertragstext zur Verfügung gestellt.

3.3.2.2. Schulen in öffentlicher Trägerschaft in Hessen

Auch das HDSG als allgemeines Gesetz zum Datenschutz für Schulen in Hessen enthält keine Vorschriften, die eine externe Speicherung von Schüler-, Eltern- oder Lehrerdaten durch Diensteanbieter generell untersagen würden. Zu beachten ist jedoch, dass das Hessische Schulgesetz in den §§ 83 bis 85 bereichsspezifische Regelungen zum Schuldatenschutz an öffentlichen Schulen in Hessen enthält.
In § 83 Abs. 7 Hessisches Schulgesetz heißt es dabei:

> „Die automatisierte Verarbeitung personenbezogener Daten darf in der Schule nur mit schuleigenen Datenverarbeitungsgeräten erfolgen, es sei denn, dass die Beachtung der erforderlichen Datensicherheitsmaßnahmen gewährleistet ist."

Grundsätzlich muss damit zwar die Verarbeitung und damit auch die Speicherung personenbezogener Daten innerhalb der Schule erfolgen. Der Gesetzgeber hat jedoch zugleich die Möglichkeit einer externen Speicherung im Weg der Auftragsverarbeitung vorgesehen. Anderenfalls wäre § 83 Abs. 7 2. Halbsatz des Hessischen Schulgesetzes überflüssig. Dies erscheint auch deswegen sinn- voll, weil eine den gesetzlichen Anforderungen entsprechende Auftragsverarbeitung aufgrund der damit verbundenen Datensicherheitsmaßnahmen grundsätzlich ein vergleichbares Schutzniveau bietet wie eine Speicherung in der Schule selbst.

Es ist daher davon auszugehen, dass auch bei öffentlichen Schulen in Hessen eine Auslagerung der Speicherung des SWOP auf einen externen Hosting-Provider grundsätzlich dann zulässig ist, wenn dabei die gesetzlichen Anforderungen an die Auftragsverarbeitung eingehalten werden. Diese er- geben sich für öffentliche Schulen in Hessen aus § 4 HDSG. Da auch die darin enthaltenen Regelungen grundsätzlich keinen über Art. 28 f., 32 DS-GVO hinausgehenden Regelungsgehalt aufweisen, gelten die Ausführungen oben unter Ziff. 3.3.2.1 entsprechend.

3.3.2.3 Schulen in freier Trägerschaft

Auf Schulen in freier Trägerschaft finden die Datenschutzbestimmungen der Schulgesetze der Länder Nordrhein-Westfalen und Hessen grundsätzlich keine Anwendung (vgl. § 6 Abs. 2 Schulgesetz NRW; § 167 Abs. 1 Hessisches Schulgesetz sowie: Der Hessische Datenschutzbeauftragte, Datenschutz in Schulen, 2010, 8).
Mangels anderweitiger Vorschriften unterliegt die externe Speicherung des SWOP bei Schulen in freier Trägerschaft in Nordrhein-Westfalen und Hessen daher den allgemeinen rechtlichen Datenschutzbestimmungen, so dass eine Auslagerung unter den Voraussetzungen der Art. 28 f., 32 DS- GVO grundsätzlich zulässig wäre. Insoweit gelten die Ausführungen unter Ziff. 3.3.2.1 auch hier.

3.3.2.4 Schulen in der Trägerschaft der evangelischen Kirche

Mangels besonderer Regelungen im Kirchengesetz über die Evangelischen Schulen findet bei Schulen in evangelischer Trägerschaft für die Frage nach der Zulässigkeit einer externen Speicherung von Schuldaten bei einem Hosting-Provider ausschließlich das allgemeine Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (im Folgenden „DSG-EKD") Anwendung. Etwaige Begrenzungen einer Auftragsverarbeitung bei der externen Speicherung von Schuldaten sind dem DSG-EKD nicht zu entnehmen, vgl. § 30 Abs. 2 DSG-EKD.

Eine entsprechende Auslagerung ist daher grundsätzlich dann zulässig, wenn diese den Anforderungen an § 6 DSG-EKD entspricht. Mit Ausnahme kleinerer kirchenrechtsspezifischer Besonderheiten orientiert sich dieser eng an die Re- gelungen der DS-GVO. Ein Vertragsmuster zur Auftragsverarbeitung zwischen Schule und Smart- Komm kann sich daher auch in diesem Fall grundsätzlich an den Vorgaben der DS-GVO orientieren und wäre nur in einigen wenigen Punkten an das geltende Kirchenrecht anzupassen. Gleiches gilt dann entsprechend für die Vereinbarung zwischen SmartKomm und dem Hosting-Provider.

3.3.2.5. Schulen in der Trägerschaft der katholischen Kirche

Kirchliche Schulgesetze für Schulen in katholischer Trägerschaft werden grundsätzlich von dem jeweiligen Erzbistum erlassen, so dass der diesbezügliche Regelungsrahmen abhängig ist vom Standort der Schule. Betrachtet man aber beispielhaft etwa die Vorschriften des Kirchlichen Schulgesetzes für das Erzbistum Köln (im Folgenden „SchulG-EBK") so ist festzustellen, dass dieses auch Regelungen zum Datenschutz enthält, vgl. §§ 42 bis 44 SchulG-EBK.

In § 42 Abs. 3 Satz 3 SchulG-EBK ist dabei vorgesehen, dass personenbezogene Daten von Schülern und deren Eltern in der Regel nur in der Schule verarbeitet werden dürfen. Im Umkehrschluss be- deutet dies, dass eine Verarbeitung und damit auch eine externe Speicherung von Schuldaten nicht generell ausgeschlossen ist. Im Übrigen verweist § 42 Abs. 1 SchulG-EBK auf die „Anordnung über den kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen in freier Trägerschaft des Erzbistums Köln (im Folgenden „KDO-Schulen"). Diese enthält zwar in §§ 3 und 8 KDO-Schulen eine Reihe von Anforderungen an die Datensicherheit bei der Verarbeitung von Schuldaten. Die diesbezüglichen Anforderungen decken sich allerdings im Wesentlichen mit denjenigen Anforderungen, die auch bei einer Auftragsverarbeitung nach Maßgabe des allgemeinen Datenschutzrechts der katholischen Kirche

in § 29 des Gesetzes über den kirchlichen Datenschutz (im Folgenden „KDG“) eingehalten werden müssen.

Geht man davon aus, dass die übrigen Erzbistümer vergleichbare Regelungen verabschiedet haben, lässt sich daher mit guten Argumenten die Auffassung vertreten, dass eine Auslagerung von Schuldaten auf einen externen Dienst- leister zulässig ist, wenn hierbei § 29 KDG entsprochen wird. Da dieser wiederum mit Art. 28 DS- GVO in wesentlichen Bereichen deckungsgleich ist, empfiehlt es sich, für SmartKomm auch die Mustervereinbarung zur Auftragsverarbeitung mit Schulen in katholischer Trägerschaft an den Regelungen der DS-GVO auszurichten. Insoweit bedarf es allerdings für jedes Bistum einer gesonderten Prüfung, ob sich aus den dortigen datenschutzrechtlichen Bestimmungen ein abweichender Regelungsbedarf ergibt.

4. Zusammenfassung und Empfehlungen

- Trotz etwaiger technischer und organisatorischer Maßnahmen zum Schutz vor einem Datenzugriff durch den Hosting-Provider ist aus Gründen der Risikovorsorge davon auszugehen, dass eine Speicherung von Daten von Schülern, Eltern und Lehrern auf Servern eines Hosting-Providers der datenschutzrechtlichen Legitimation bedarf (siehe dazu Ziff. 3.1).

- Verantwortlicher für eine rechtskonforme Speicherung der Daten der Betroffenen beim Hosting-Provider ist in Bezug auf die Funktionen des SWOP als Sozialem Netzwerk Smart- Komm. Für die Speicherung von Daten der Betroffenen beim Hosting-Provider zu Zwecken der Schulverwaltung trägt die jeweilige Schule die datenschutzrechtliche Verantwortung (siehe dazu Ziff. 3.2).

- Soweit SmartKomm verantwortliche Stelle für die Speicherung der Daten beim Hosting- Provider ist, ist davon auszugehen, dass der Hosting-Provider insoweit als Auftragnehmer einer Auftragsverarbeitung für SmartKomm tätig wird. Die Datenspeicherung lässt sich in diesem Fall durch den Abschluss einer Vereinbarung zur Auftragsverarbeitung zwischen SmartKomm und dem Hosting-Provider sowie durch technisch-organisatorische Kontrollmaßnahmen im Sinne von Art. 32 DS-GVO legitimieren (siehe dazu Ziff. 3.3.1.2).

- Soweit Schulen im Hinblick auf die Nutzung des SWOP dieses zur Schulverwaltung nut- zen, ist eine Auslagerung der Daten auf Server des Hosting-Providers – unabhängig von der jeweiligen Schulform – ebenfalls grundsätzlich im Wege der Auftragsverarbeitung zu- lässig. Auftragnehmer wäre dabei SmartKomm, die wiederum einen Subunternehmervertrag mit dem Hosting-Provider schließen müsste. Bei entsprechender Ausgestaltung könnte dabei ein einheitliches Vertragsdokument entworfen werden, das sowohl die un- mittelbare Auftragsverarbeitung des Hosting-Providers gegenüber SmartKomm als auch seine Funktion als Subunternehmer im Auftragsverhältnis zwischen Schule und Smart- Komm abdeckt (siehe dazu Ziff. 3.3.2).