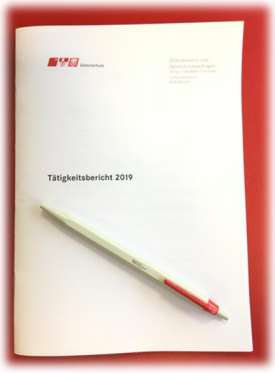
DATENSCHUTZ AKTUELL

01. Juli 2020

(Öffentlichkeits- und)
Datenschutzbeauftragter
Schwyz - Obwalden - Nidwalden

Jahrgang 2020, Ausgabe 1

In dieser Ausgabe:



Editorial

Geschätzte Leserinnen und Leser

Die letzte Zeit wurde vor allem von Informationen zu COVID-19 beherrscht. Auch wir blieben davon nicht verschont und durften uns mit neuen Themen auseinandersetzen.

Darum finden Sie in diesem Newsletter einen Artikel mit Verhaltenstipps für Personen, die «im Homeoffice» arbeiten. Was muss man bei der Arbeit zu Hause beachten?

In einer Zusammenfassung unseres Tätigkeitberichts 2019 zeigen wir auf, was uns letztes Jahr beschäftigte. Daraus ist ersichtlich, wieviel Aufwand wir für welche unserer Tätigkeiten (Kontrolle, Beratung, Gesetzgebung, Kurse etc.) erbrachten.

In drei Fällen aus unserer Praxis beantworten wir die Fragen: Welche Daten dürfen Schulen an Kirchen bekannt geben? Wie sollen Passwörter von Schulen (z.B. zur Nutzung von Office 365) den Schülern mitgeteilt werden? Wie sind Zahlungsbefehle zuzustellen?

Für Ihr Interesse danken wir bestens und freuen uns über Ihre Rückmeldungen.

Philipp Studer

Hier können Sie unsere News (u. a. „DATENSCHUTZ AKTUELL") abonnieren:
http://www.kdsb.ch/xml_1/internet/de/application/d12/f17.cfm

Tätigkeitsbericht 2019: Es braucht Datenschutz!

Im Jahr 2019 waren Beratung, Kontrollen und Sensibilisierung zentral. Dabei ergab sich: Digitalisierung braucht Vertrauen und Datenschutz schafft Vertrauen. Deshalb braucht es Datenschutz.

Als (Öffentlichkeits- und) Datenschutzbeauftragter der Kantone Schwyz, Obwalden und Nidwalden (ÖDB) sind wir zur Beurteilung von Datenbearbeitungen durch öffentliche Organe in diesen Kantonen zuständig. Deren Datenschutzgesetze verpflichten uns zur jährlichen Berichterstattung über unsere Tätigkeiten an unsere Aufsichtsbehörden (SZ & OW: Kantonsrat; NW: Regierungsrat). Diese nehmen ihn zur Kenntnis.

Datenschutz schafft Vertrauen

Datenschutz ist Schutz unserer Persönlichkeit und somit unserer Privatsphäre. Datenschutz gewährleistet den korrekten Umgang mit den Daten aller Personen. Ein eigentlich typisches demokratisches und urliberales Anliegen.

Im Tätigkeitsbericht 2019 erwähnen wir, wie wir öffentliche Organe durch Beratung, Kontrollen und Sensibilisierung unterstützten, so dass sie mit den ihnen anvertrauten Daten von Bürgerinnen und Bürgern (Bürger) korrekt umgehen. Gerade in der heutigen Zeit, in der Digitalisierung «grossgeschrieben» wird, müssen öffentliche Organe mit den ihnen anvertrauten Daten der Bürger äusserst sorgfältig umgehen. So können sie gegenüber der Bevölkerung mit der Einhaltung der Datenschutzvorgaben grösseres Vertrauen erwirken.

Digitalisierung braucht Vertrauen.
Datenschutz schafft Vertrauen.

Aufsicht & Kontrolle

Ein Grossteil des Kontrollaufwands fiel 2019 auf die Kontrolle der Umsetzung der in den Kommunaluntersuchen und Datenschutzreviews bei Gemeinden und Bezirken der Vereinbarungskantone ausgewiesenen Pendenzen Diese begannen wir bereits 2018 und konnten im Berichtsjahr einiges erreichen.

2019 schlossen wir die Kontrolle der Nutzung des Schengener Informationssystems (SIS) bei der Kantonspolizei Schwyz mit der Nachbesprechung bei der Polizei ab. Zu denselben Kontrollen in Ob- und Nidwalden erstellten wir die Berichte.

Zudem aktualisierten wir die Übersicht der von öffentlichen Organen betriebenen Videoüberwachungskameras. Dabei gab es aufgrund der erhaltenen Rückmeldungen und bei anstehenden Projekten im Voraus gewisse Fragen zu klären.

Daneben führten wir verschiedene Kontrollen durch. So überprüften wir z.B. auf Anfrage der Finanzkontrolle des Kantons Schwyz mit dieser zusammen das Personalamt Schwyz. Weiter bearbeiteten wir einzelne Anzeigen und Meldungen von Privaten.

Beratung & Unterstützung

Die Beratung öffentlicher Organe und Privater ist sehr wichtig. Sie stellte auch 2019 den grössten Teil unserer Tätigkeit dar (knapp 33% der Geschäftslast). Es besteht also weiterhin und aufgrund immer neuer Themen ein grosser Informationsbedarf. So gingen bei uns im Berichtsjahr insgesamt 322 Anfragen von öffentlichen Organen und Privaten ein (22 mehr als 2018). Davon stellten 192 Kleinanfragen dar, die wir rasch (teilweise direkt am Telefon) beantworten konnten.

Wir berieten im Berichtsjahr verschiedene Personen und Behörden zu u.a. folgenden Themen: ...

Bildquelle: Cornerstone / pixelio.de

Versand von E-Mails, Verwendung von Cloud-Lösungen, Videoüberwachung, Amtshilfe, Datenschutz an Schulen, Publikation von Personendaten (z.B. auf Webseiten), Öffentlichkeitsprinzip oder Einsichts- und Auskunftsrecht.

Gesetzgebung

Im Berichtsjahr nahmen wir zu 19 von 25 erhaltenen Vorlagen Stellung. Die schon 2018 festgestellte Tendenz zu umfangreicheren und komplexeren Vorlagen bestätigte sich auch 2019. Zentral waren u.a. folgende Vorlagen: Revision kantonaler Datenschutzgesetze, Änderung DNA-Profil-Gesetz (Bund), Adressdienstgesetz (Bund), Revision Polizeigesetz (SZ), Vorarbeiten zur Einführung des Öffentlichkeitsprinzips (OW & NW).

Schulung & Information

Wir führten 2019 sieben Schulungen und drei Referate zur Sensibilisierung diverser Personen und Stellen durch. In allen Vereinbarungskantonen hielten wir einen Kurs zum Datenschutz. Im Kanton Schwyz zudem einen für die Lernenden der Kantonsverwaltung und einen zum Öffentlichkeitsprinzip. Neu hielten wir am Zentralschweizer Praktikantenkurs, an dem künftige RechtsanwältInnen aus der Zentralschweiz teilnehmen können, eine Schulung zum Datenschutz und Öffentlichkeitsprinzip. Im Kanton Obwalden zeigten wir Lehrpersonen in einem spezifischen Kurs für die Schule relevante Bereiche und deren Umsetzung in der Praxis auf.

Weiter sensibilisierten wir 2019 die Mitarbeitenden der Polizei Obwalden mit einem Referat zur Nutzung des SIS (welche Abfragen dürfen darin getätigt werden?) sowie im Kanton Schwyz die Spitalkonferenz zum Datenschutz und der Datensicherheit an Spitälern.

Datenschutz schützt die Privatsphäre von uns allen. Der Staat darf nur die zur Erfüllung seiner gesetzlichen Aufgaben notwendigen Daten der Bürgerinnen und Bürger bearbeiten.

Neben dem Tätigkeitsbericht informierten wir mit zwei Ausgaben unseres Newsletters *„DATENSCHUTZ AKTUELL“*, über unsere Webseite (z.B. in der neuen Rubrik «Ihre Rechte») und beantworteten verschiedene Medienanfragen.

Zusammenarbeit & Organisation

In der Koordinationsgruppe Schengen, der Arbeitsgruppe Öffentlichkeitsprinzip und bilateral mit anderen Beauftragten pflegten wir eine wertvolle Zusammenarbeit.

Das Budget wurde auch 2019 eingehalten. Die Personaldotierung von 180 Stellenprozenten und die zunehmende Arbeitslast mit immer komplexeren Fragen stellen uns weiterhin vor Probleme. Im Bereich Informatik besteht das bekannte Know-How-Defizit, das in Zukunft durch die Anstellung einer IT-Fachperson minimiert werden soll.

Fazit

Es braucht einen wirksamen Datenschutz; erst recht bei der unaufhaltsam voranschreitenden Digitalisierung. Dies zeigt sich in der hohen Anzahl uns gestellter Anfragen und gilt unabhängig davon, wie sich Bürger selber in den sozialen Medien verhalten, auch wenn einige dort auf Datenschutz zu verzichten scheinen!

Datenschutz ist also kein notwendiges Übel, das den Datenaustausch verbietet und die Arbeit behindert. Vielmehr gewährleistet er den Schutz unserer Persönlichkeit bzw. unserer Privatsphäre und schafft dadurch Vertrauen bei Bürgerinnen und Bürgern.

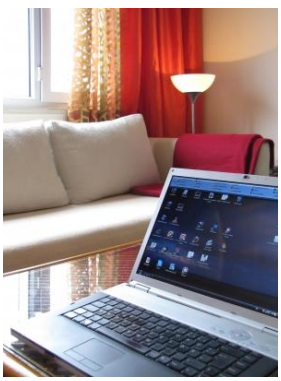
Philipp Studer

„Nur kluge Fürsten können klug beraten werden.“

© Niccoló Machiavellli (1469-1527), italienischer Staatsmann und Schriftsteller

Den Tätigkeitsbericht 2019 finden Sie unter:
https://www.kdsb.ch/xml_1/internet/de/application/d144/f146.cfm

Wie hast du‘s mit dem Homeoffice?



Bildquelle: Rainer Sturm / pixelio.de

Diese «Gretchenfrage» stellt sich seit dem Auftauchen von Covid-19 häufiger. Einige Personen wurden und werden dadurch zur Arbeit im Homeoffice verpflichtet. Diese immer noch relativ neue Arbeitsform wirft Fragen auf: Sei es im Arbeitsrecht, bezüglich der Wahrung von Amts-, Geschäfts- und Berufsgeheimnissen sowie der Einhaltung von Datenschutz- und Datensicherheitsvorgaben.

Was gilt es für Arbeitnehmende bei öffentlichen Organen im Homeoffice zu bedenken?

Vereinbarung und Weisungen

Grundsätzlich ist jedes öffentliche Organ, welches Personendaten bearbeitet, für deren Schutz verantwortlich. Homeoffice wird meist vertraglich geregelt (z.B. zusätzliche Geheimhaltungsvereinbarungen, Modalitäten). Die Arbeitgeber bzw. das verantwortliche öffentliche Organ erlassen ausserdem Vorgaben und Weisungen, wie mit den Daten im Homeoffice umzugehen ist.

Im Büro wird alles vor Ort bearbeitet, gespeichert und abgelegt und die Mitarbeitenden sind persönlich anwesend. Dann ist die Verantwortung und Kontrolle des Arbeitgebers leichter wahrzunehmen als wenn Mitarbeitende zu Hause arbeiten.

Sind Sie entsprechend für das Homeoffice geschult worden? Kennen Sie Ihre Rechte und Pflichten? Haben Sie entsprechende Vereinbarungen unterschrieben? Fragen Sie im Zweifel und bei Unklarheiten bei Ihrem Vorgesetzten nach.

Arbeiten unterwegs

Auch wenn telefonieren und arbeiten in unserer mobilen Gesellschaft grundsätzlich an immer mehr Orten möglich ist: Geschäftliche Anrufe im Zug sind keine gute Idee. Jeder Reisende kann mithören und so gewisse Geheimnisse und/oder Namen erfahren. Genauso verhält es sich auch auf der Strasse, in Parks oder wo auch immer unberechtigte Personen mithören oder -sehen können. Gewährleistet ein Sichtschutz, dass nur Sie den Bildschirm sehen können? Ist das Display nicht in einem Spiegel oder Fenster für andere sichtbar?

Lassen Sie Ihre Geräte im öffentlichen Verkehr oder an öffentlichen Orten niemals unbeaufsichtigt. Auch wenn es mühsam ist: Nehmen Sie ihr Notebook mit, falls Sie ihren Platz aus irgendwelchen Gründen verlassen müssen. So können Sie sich vor Gerätediebstahl und/oder Datenmissbrauch schützen und nehmen Ihre Verantwortung wahr.

Arbeitsplatz im Homeoffice

Stellen Sie sicher, dass Dokumente und Unterlagen sowie portable Datenträger unzugänglich und von privaten Unterlagen getrennt aufbewahrt werden. Je nach Anzahl Personen, die mit Ihnen zusammenwohnen, sowie von ...

Einrichtung/Platzverhältnissen, gestalten sich die Massnahmen anders. Nicht alle Personen haben ausreichend Raum für das Homeoffice und müssen sich in der Notlage entsprechend arrangieren und privaten Platz für ein provisorisches Büro «opfern». Am idealsten ist ein separates, abschliessbares Büro und Mobiliar sowie die Aktivierung des Sperrbildschirms, sobald der Arbeitsplatz verlassen wird. Schreddern Sie Dokumente oder entsorgen Sie diese auf andere Weise fachgerecht. Legen Sie keine Dokumente ins Altpapier. Halten Sie die Fenster immer geschlossen, wenn Sie sich nicht an Ihrem Arbeitsplatz befinden.

Achten Sie im Freien, z.B. auf dem Balkon darauf, dass Nachbarn oder Passanten auf keinen Fall Ihre geschäftlichen Gespräche mithören können. Dies gilt auch innerhalb der «eigenen vier Wände». Vermeiden Sie, dass Ihre Familie, Partner und Partnerinnen, Personen aus der WG oder Besucher und Besucherinnen Zugang zu Geschäftsdaten erhalten können. Erklären Sie ihnen «publikumsgerecht» die Situation. Partnern und Partnerinnen muss allenfalls erklärt werden, dass Ihre Arbeit (z.B. Unterlagen, Gespräche) dem Amts- und/oder Berufsgeheimnis sowie dem Datenschutz unterstehen und nicht vom familiären Vertrauensbereich erfasst sind (selbst wenn sich amtliche Unterlagen im persönlichen Lebensraum befinden).

Firmengeräte und Software/Dienste

Auch bezüglich Geräten und Software empfiehlt sich aus Sicherheitsgründen die Verwendung separater Geräte. Arbeitsgeräte (Notebooks, Drucker, Telefonie, Speichermedien) haben grundsätzlich vom Arbeitgeber zur Verfügung gestellt und konfiguriert zu werden. Es soll nur durch das öffentliche Organ bzw. die IT-Abteilung auf Datenschutz und –sicherheit geprüfte Software, Services und Dienste verwendet werden. Dies gilt insbesondere für Kommunikations- und Konferenzsoftware. Andernfalls bestehen grosse Datenschutz- und Datensicherheitsrisiken.

Berufliche und private Daten sollen stets getrennt bleiben. Verwenden Sie Ihre privaten Geräte (wie auch Nummern und Adressen) für private Zwecke und Daten, die Firmengeräte hingegen für geschäftliche Zwecke und Arbeitsdaten. Bring your own device ist möglichst zu vermeiden.

Mit Firmengeräten kann gewährleistet werden, dass der Arbeitgeber seine Kontrollrechte in einer Weise ausüben oder die Verwendung von Software vorschreiben kann, ohne Ihre Privatsphäre oder persönliche Freiheit auch in Ihrer Freizeit zu beeinträchtigen (Webseitesperren, Kontrollmöglichkeiten, Fernlöschungen, Installation von bestimmten Diensten/Programmen, Zugriff auf Daten aller Art, usw.).

Homeoffice erfordert grosse Verantwortung.

Wird die Trennung von Beginn weg konsequent beachtet, entstehen später weniger Aufwand und Probleme. Die Firmengeräte gehen bei Beendigung von Homeoffice und/oder des Arbeitsverhältnisses zurück an das öffentliche Organ und werden dort professionell neu aufgesetzt oder entsorgt. Separat abgelegte und sicher aufbewahrte Akten werden wieder mitgenommen und entsprechend im Büro abgelegt.

Technische Vorgaben

Halten Sie sich an die technischen Vorgaben Ihres Arbeitgebers und der IT. Es sollte ein Passwortgeschütztes WLAN genutzt werden und sich über eine VPN-Verbindung ins Netzwerk eingewählt werden. Natürlich gelten die regulären Vorgaben wie Passwort- oder Virenschutzbestimmungen sowie Anordnungen zum Mailversand (z.B. verschlüsselter Versand von Personendaten) auch im Homeoffice.

Angriffsziel Homeoffice

Im Homeoffice sind die Risiken bezüglich Cyberattacken grösser. Dies wird von Cyberkriminellen ausgenutzt. Einerseits haben IT-Abteilungen weniger Kontrolle über die Sicherheit von Geräten und Netzen, andererseits werden Angriffe (z.B. Phishing) später entdeckt, da der Austausch zwischen den Mitarbeitenden geringer ist (Information, Hilfe). Melden Sie Vorfälle, damit die entsprechenden Massnahmen getroffen werden können. Denken Sie auch an analoge Gefahren wie Einbruch und oder Diebstahl.

Fazit: Grosse Verantwortung

Sie als Arbeitnehmende im Homeoffice haben eine grosse Eigenverantwortung, sich an die Regeln zu halten.

Wenn Sie Fragen haben, sprechen Sie mit Ihrem Arbeitgeber. So können die bestehenden Vereinbarungen und Weisungen allenfalls erweitert oder genauer spezifiziert werden, damit die Datenschutz- und Datensicherheitsvorgaben bestmöglich sichergestellt sind.

Sonja Burkart

Bildquelle: Stefan Bayer / pixelio.de

„Gutes Werkzeug, halbe Arbeit.“

© aus Ungarn

„Aus der Praxis“

Darf eine Schule der Kirche Daten über Schülerinnen und Schüler (SuS) bekannt geben?

Generell gesehen findet sich in der Schulgesetzgebung keine Grundlage für eine Datenbekanntgabe der Schule an die Kirche.

Die Kirchen erhalten gemäss § 4 der Verordnung über das Einwohnermeldewesen aus den Einwohnerregistern (und nicht von den Schulen) folgende Daten über ihre Mitglieder:

«[1] Die Kirchgemeinden erhalten über ihre Mitglieder die Daten über Namen, Ledignamen, Vornamen, Adresse, Geburtsdatum, Geburtsort, Heimatort, Zivilstand, Staatsangehörigkeit, Aufenthaltsstatus, Zuzug, Umzug, Wegzug und Todesfall.

[2] Hat das Mitglied das 16. Altersjahr noch nicht zurückgelegt, so umfasst die Datenbekanntgabe zudem Name, Vorname und Adresse der Inhaber der elterlichen Sorge.»

Aber: Wie verhält es sich, wenn es die Planung des Religionsunterrichts betrifft?

Die Weisungen über die Unterrichtsorganisation an der Volksschule halten fest, dass die Kirche als Körperschaft des öffentlichen Rechts für die Organisation, Planung und Finanzierung des konfessionellen Religionsunterrichts zuständig ist.

Gemäss § 9 Abs. 2 Bst. a des Gesetzes über die Öffentlichkeit der Verwaltung und den Datenschutz des Kantons Schwyz (ÖDSG) dürfen besonders schützenswerte Personendaten nur bearbeitet werden, wenn dies für die Erfüllung einer gesetzlichen Aufgabe zwingend erforderlich ist. Nach § 14 Bst. b ÖDSG kann der Datenempfänger dartun, dass er zur Bearbeitung der verlangten Personendaten berechtigt ist und der Bekanntgabe keine Geheimhaltungspflicht entgegensteht. Demzufolge darf eine Schule für die Planung des konfessionellen Religionsunterrichts die dazu zwingend erforderlichen Personendaten der SuS aus den einzelnen ...

Bildquelle: Kantonsschule Kollegi Schwyz

Bildquelle: S. Hofschlaeger / pixelio.de

Klassen bekannt geben. Im Rahmen des Verhältnismässigkeitsprinzips dürfen es nicht mehr Daten sein, als für die Planung erforderlich sind; aber so viel wie nötig, damit die Aufgabe erfüllt werden kann.

Da es sich um einen konfessionellen Religionsunterricht handelt, dürfen nur Daten der SuS weitergegeben werden, welche der entsprechenden Konfession angehören und nicht eine Liste aller SuS. Die Kirche muss aber wissen, welche SuS aus welcher Klasse wann und wo den Religionsunterricht besuchen könnten, damit sie den Unterricht planen und durchführen kann.

DSB SZ-OW-NW

Darf der zustellende Postbote wissen, dass ich betrieben werde?

Konkret hatte eine Person unter anderem diese und andere Fragen zur Zustellung eines Zahlungsbefehls. Die Antwort findet sich im Bundesgesetz über Schuldbetreibung und Konkurs (SchKG).

Gemäss Art. 72 Abs. 1 SchKG geschieht die Zustellung der Zahlungsbefehle durch den Betreibungsbeamten, einen Angestellten des Amtes oder durch die Post. Art. 72 Abs. 2 SchKG hält fest, dass der Überbringer auf beiden Ausfertigungen bescheinigen muss, an welchem Tage und an wen die Zustellung erfolgt ist.

Der Zahlungsbefehl ist zu übergeben, die Zustellung durch einfachen oder eingeschriebenen Brief ist unzulässig. Grund dafür ist die einfache Eröffnung eines Betreibungsverfahrens. Die betriebene Person soll mit Sicherheit von der Betreibung Kenntnis erhalten und allenfalls Rechtsvorschlag erheben können.

Erfolgt die Zustellung des Zahlungsbefehls durch die Post, so handeln die entsprechenden Postangestellten als Betreibungsgehilfen. Die Postangestellten unterstehen dem Amts- und Post- bzw. Briefgeheimnis.

Übrigens: Beim Zahlungsbefehl gibt es keine fingierte Zustellung. Wird einer Abholungseinladung im Briefkasten nicht Folge geleistet, so gilt der Zahlungsbefehl nicht automatisch am letzten Tag der Abholung als empfangen. Bleiben die Zustellungsversuche weiterhin erfolglos, kann die Zustellung ultima ratio durch eine öffentliche Bekanntmachung (!) ersetzt werden, wenn sich der Schuldner beharrlich der Zustellung entzieht (Art. 66 Abs. 4 Ziff. 2 SchKG).

DSB SZ-OW-NW

„Eine Wolke entzieht sich der Planbarkeit.“

© Peter Cerwenka (*1942), Univ.-Prof. a. D. Dr., Fachbereicht Verkehrssystemplanung, Technische Universität Wien

Wie soll die Schule den Schülerinnen und Schülern (SuS) bzw. deren Eltern die Passwörter zur Nutzung neuer Cloud-Lösungen (z.B. Office 365) in der «Corona-Zeit» mitteilen?

Im März 2020 beschloss der Bundesrat, dass Schulen bis auf weiteres geschlossen werden müssen. Damit die SuS zu Hause ihre Aufgaben erledigen und bei Bedarf mit anderen SuS und/oder Lehrpersonen kommunizieren konnten, mussten neue Anwendungen eingeführt werden. Wie sollten den SuS die Zugangsdaten am besten mitgeteilt werden (z.B. per Post, E-Mail, Whatsapp oder persönlicher Übergabe an SuS)?

Ein Versand per Whatsapp ist aufgrund der automatischen Bekanntgabe sämtlicher auf dem Smartphone vorhandenen Kontaktangaben nicht erlaubt. Persönliche Übergaben können zu einem grossen Aufwand seitens Schule (Koordination der Abholungen) führen, weshalb gewisse Schulen davon absahen, obwohl dies eine gute Variante gewesen wäre.

Grundsätzlich ist der normale (d.h. unverschlüsselte) E-Mail-Versand unsicher. Daneben ist zu unterscheiden, wem eine E-Mail geschickt wird und was darin enthalten ist (Sach-, Personen- oder besonders schützenswerte Personendaten).

Sobald E-Mails ausserhalb eines gegen Aussen geschützten Netzwerks (z.B. an Empfänger ausserhalb der Schule X.) versendet werden, besteht ein hohes Risiko, dass die Daten von Unberechtigten eingesehen werden können. Die Mitteilung der Zugangsdaten zu Office 365 oder anderen Anwendungen sollten SuS bzw. deren Eltern nicht unverschlüsselt auf deren private E-Mail-Adresse geschickt werden. Sonst könnten die angemessenen technischen Schutzmassnahmen gemäss Art. 7 des Datenschutzgesetzes des Kantons Nidwalden nicht eingehalten werden.

Datenträger und Dokumente (z.B. Zugangsdaten bzw. Passwörter) können auch heute noch per Post verschickt werden. In der Schweiz gilt zudem das in der Bundesverfassung und im Strafgesetzbuch verankerte «Postgeheimnis». Deshalb empfahlen wir der Schule, die Zugangsdaten den berechtigten Personen per Post (möglichst persönlich adressiert) zuzustellen.

DSB SZ-OW-NW

(Öffentlichkeits- und) Datenschutzbeauftragter
Schwyz - Obwalden - Nidwalden

Gotthardstrasse 21
6414 Oberarth

Telefon 041 859 16 20
Fax 041 859 16 26
E-Mail: info@kdsb.ch
www.kdsb.ch