DATENSCHUTZ FÜR DIE SCHULE

Ein praxisorientierter Leitfaden von IServ


iserv
WIR DIGITALISIEREN
DEINE SCHULE
IN45MINUTEN.DE
Jetzt kostenfrei testen

INHALTSVERZEICHNIS

DATENSCHUTZ FÜR DIE SCHULE

Ein praxisorientierter Leitfaden von IServ

Bei der Schuldigitalisierung führt kein Weg am Thema Datenschutz vorbei. Dort, wo die sensiblen und personenbezogenen Daten von Schülerinnen und Schülern gespeichert und weiterverarbeitet werden, gilt eine besondere Sorgfaltspflicht.

Oftmals ist in diesem Zusammenhang davon die Rede, dass sich Schuldigitalisierung und Datenschutz gegenseitig behindern würden. Dem möchten wir entschieden widersprechen! Schuldigitalisierung und Datenschutz gehen Hand in Hand. Datenschutz verhindert nicht die Digitalisierung von Schulen. Sie ist eine Grundvoraussetzung, um das Vertrauen aller beteiligten Nutzerinnen und Nutzer zu gewinnen und so die Digitalisierung unserer Schulen insgesamt voranzubringen.

Schon jetzt stellen wir mit IServ an über 5.000 Schulen eine vielseitige datenschutzkonforme Software-Lösung zur Schuldigitalisierung bereit. Damit sind wir bundesweit Marktführer im Bereich »digitale Schulplattform« und bewerkstelligen diese Herausforderung täglich mit unserem stetig wachsenden Team von derzeit mehr als 150 Kolleginnen und Kollegen an bundesweit drei Standorten.

Datenschutz verhindert nicht die Digitalisierung von Schulen. Sie ist eine Grundvoraussetzung, um das Vertrauen aller beteiligten Nutzerinnen und Nutzer zu gewinnen und so die Schuldigitalisierung insgesamt voranzubringen.«

Jörg Ludwig – Gründer und Geschäftsführer der IServ GmbH

Damit auch Sie Ihre Schule so niederschwellig wie möglich datenschutzkonform digitalisieren können, haben wir die wichtigsten Fragen zum Thema Datenschutz für Sie zusammengetragen und in dem nun vorliegenden praxisorientierten Leitfaden »Datenschutz für die Schule« aufbereitet.

Wir klären für Sie aufeinander aufbauend elementare Fragen wie: Welche Rolle spielt Datenschutz für unsere Schulen? Was ist eine Auftragsverarbeitung? Welche Anforderungen stellt der Datenschutz? Wo wird schulische IT geregelt? Dabei zeigen wir Ihnen mögliche Fallstricke bei der Umsetzung auf.

Viel Spaß beim Lesen

Ihr IServ Team

WELCHE ROLLE SPIELT DER DATENSCHUTZ IN UNSEREN SCHULEN?

WAS BEDEUTET DATENSCHUTZ FÜR SCHULEN?

Unsere Schulen werden immer digitaler. Die Daten von Schülerinnen und Schülern, Lehrkräften und Eltern werden in Programmen und Systemen erfasst und für die schulischen Prozesse verarbeitet. Es werden Daten erzeugt, die sich konkret auf eine bestimmte Person beziehen und über diese Person Auskunft geben können. Es handelt sich um sogenannte personenbezogene Daten, für die ein Schutzbedürfnis und ein Selbstbestimmungsrecht entstehen. Keiner möchte, dass diese Daten beliebig bearbeitet, gespeichert, eingesehen oder weitergegeben werden können oder gar, dass Handel mit ihnen getrieben wird.

Für dieses umfassende Schutzbedürfnis und Selbstbestimmungsrecht steht der Datenschutz, der immer personenbezogen ist und im Kern den Schutz der Person selbst meint. Konkret geht es beim Datenschutz in der Schule um alle am schulischen Prozess beteiligten Personen, also neben den Schülerinnen und Schülern, den Lehrkräften z. B. auch um die Eltern und das Personal der Schulverwaltung.

Dabei sind insbesondere Schülerdaten in mehrfacher Hinsicht hochsensibel. Schließlich handelt es sich um personenbezogene Daten von überwiegend Minderjährigen. Ihre Daten unterliegen allein schon deshalb einem besonderen Schutz.

WO IST DATENSCHUTZ GEREGELT?

Der Datenschutz ist in der EU 2018 neu geregelt worden. In Deutschland heißt die Umsetzung der EU-Normen »Datenschutzgrundverordnung« oder kurz »DSGVO«. In der DSGVO werden verschiedene Dimensionen des Datenschutzes berücksichtigt und abgebildet.

Es geht um
- den Schutz vor Datenmissbrauch,
- das Recht auf informationelle Selbstbestimmung,
- den Schutz der Persönlichkeitsrechte sowie
- den Schutz der Privatsphäre.

WAS IST EINE AUFTRAGSVERARBEITUNG?

Für die rechtliche Umsetzung der DSGVO an Schulen sind in Deutschland die Bundesländer verantwortlich. Sie interpretieren die Datenschutzgrundsätze der DSGVO für den Bereich »Schule« und definieren über die Landesdatenschutzgesetze, die Schulgesetze und Verordnungen den rechtlichen Rahmen.

WER IST FÜR DATENSCHUTZ VERANTWORTLICH?

Die konkrete Umsetzung der Datenschutzbestimmungen obliegt den Schulen. Sie müssen den Datenschutz in die schulischen Abläufe integrieren und sicherstellen, dass kein Missbrauch stattfindet.

Wichtig: Verantwortlich und rechenschaftspflichtig für den Datenschutz an Schulen ist die jeweilige Schulleitung.

WAS VERSTEHT DER DATENSCHUTZ UNTER PERSONENBEZOGENEN DATEN?

Aus der Datenschutzperspektive sind alle Daten personenbezogen, die sich auf eine identifizierbare Person rückführen lassen:

Name, Adresse, Telefonnummer, Geburtsdatum, Klassenbucheinträge, Noten, Beurteilungen usw. Aber auch alles, was auf diese Person schließen lässt: Meinungen, Vorlieben, Interessen, Hobbys … Wenn durch diese Daten ein Risiko für die Person erzeugt werden kann oder wenn Noten, Beurteilungen z. B. in falsche Hände kommen können, dann sind es sensible Daten. Aber das sind die Daten von Kindern und Jugendlichen ohnehin.

WAS BEDEUTET ES, PERSONENBEZOGENE DATEN ZU »VERARBEITEN«?

Oft denken wir bei der Verarbeitung von Daten an eine geschäftliche Nutzung. Also etwa ihre Weitergabe und der Verkauf an Dritte oder ihre Auswertung und Weiternutzung, wie wir sie aus dem elektronischen Handel kennen. »Verarbeiten« beschreibt aber zunächst einfach nur, was mit Daten unternommen werden kann: Sehen, Hören, Aufschreiben, Speichern, Ändern, Löschen, Drucken, Weitergeben, Auswerten etc. Ob diese Daten digital oder noch auf Papier verarbeitet werden, spielt keine Rolle.

WARUM MÜSSEN DATEN GESCHÜTZT WERDEN?

Der Grund ist einfach: Die Daten gehören der Person, auf die sie sich beziehen. Das ist wesentlich und immer zu beachten. Ein bekanntes Risiko des Datenmissbrauchs an Schulen ist z. B. das Mobbing von Mitschülerinnen und -schülern. Ein weiteres bekanntes Risiko besteht auch, wenn bspw. durch die Weitergabe von Zugangsdaten Schulrechner von außen zugänglich gemacht werden. Fehlende Schutzmechanismen beim Zugang sind eine der häufigsten Ursachen von Datenmissbrauch. Die Schule bzw. konkret die Schulleitung ist dafür verantwortlich, dass die Datenschutzrisiken durch unabsichtliches oder absichtliches Handeln von Personen oder durch fehlenden technischen Schutz minimiert werden.

Mit der Auftragsverarbeitung ist die Verarbeitung von personenbezogenen Daten durch Dritte, also externe Auftragsverarbeiter(innen), gemeint. Das können z. B. IT-Firmen sein, deren Softwareprodukt an der Schule eingesetzt wird und die im Auftrag der Schule, des Schulträgers oder der Landesbehörden arbeiten.

Ein Zugriff auf die personenbezogenen Daten durch Dritte darf nur erfolgen, wenn die Schule als verantwortliche Instanz einen Auftragsverarbeitungsvertrag (AVV) mit diesen externen Verarbeiter(inne)n abgeschlossen hat.

Mit dem AVV wird geregelt, dass auf Weisung der Schule auf die personenbezogenen Daten zugegriffen werden darf. Die Anbieter(innen) schulischer Software-Lösungen stellen den Schulen in aller Regel Entwürfe für den AVV zur Verfügung.

WELCHE ANFORDERUNGEN STELLT DER DATENSCHUTZ?

Für die konkrete Umsetzung des Datenschutzes hat die DSGVO sogenannte Datenschutzgrundsätze entwickelt. Diese Grundsätze sollen im Folgenden vorgestellt werden.

1. DIE TRANSPARENZ DER DATENNUTZUNG

Transparenz der Datennutzung bedeutet, dass eine Person immer über die Verarbeitung ihrer Daten informiert ist. Das Verzeichnis von Verarbeitungstätigkeiten (VVT) ist nur die Voraussetzung dafür, dass die Schule nachweislich den Überblick hat (z. B. über Daten, Dauer, Empfänger oder Zweck). Für die Praxis heißt das, dass die Schule einen Überblick erstellen muss, der aufzeigt, welche personenbezogenen Daten in welchen Systemen und zu welchem Zweck verarbeitet werden. Dieser Überblick muss allen Personen, deren Daten verarbeitet werden, zugänglich sein.

Um u. a. dem Transparenzgrundsatz gerecht zu werden, muss die Schule ein Verzeichnis der Verarbeitungstätigkeiten führen und auf Verlangen der Aufsichtsbehörde vorlegen. Die Schulleitung ist für das Verzeichnis verantwortlich, kann die Erstellung aber delegieren. Der Aufbau und die Inhalte des Verzeichnisses sind in der DSGVO (§ 30) beschrieben. Es umfasst alle Aspekte des personenbezogenen Datenschutzes: die Benennung der/des Verantwortlichen und der/des Datenschutzbeauftragten, die konkreten Verarbeitungszwecke, die erfassten Datenkategorien (wie z. B. Namen und Adressdaten), die Daten der internen und externen Datenverarbeiter(innen), die für die Datenverarbeitung eingesetzten Softwareprodukte, Lösch- und Speicherfristen, die Regelung der Zugriffsrechte, die betroffenen Personenkreise, die technischen und organisatorischen Maßnahmen zur Datensicherung und Zutrittskontrolle etc.

Der Aufbau des Verzeichnisses ist umfangreich und bedeutet für die Schule eine Menge Arbeit. Als IServ bieten wir mit unserem »Dokumentenpaket für Schulen« für einige Aspekte Unterstützung an: **iserv.de/downloads/privacy**

2. DAS RECHT AUF INFORMATIONELLE SELBSTBESTIMMUNG

Das Recht auf informationelle Selbstbestimmung gibt vor, dass jede Person grundsätzlich selbst darüber entscheiden darf, welche personenbezogenen Daten sie oder er von sich preisgeben möchte und wer diese verwenden darf. In der Schule wird dieses Recht durch die Schulpflicht eingeschränkt. Die Schule darf alle Daten erfassen und verarbeiten, die für den Schulbetrieb notwendig sind. Grundsätzlich sind das zunächst einmal Name und Vornamen, die Adresse und das Geburtsdatum. Die weiteren Daten, die eine Schule erheben und verarbeiten darf, sind gesetzlich geregelt. In den Schulgesetzen und Verordnungen der Bundesländer finden sich Listen mit Daten, die von den Schulen zusätzlich erhoben werden dürfen.

Sollen darüber hinaus weitere Daten, wie z. B. Fotos oder Videos von Schüler(inne)n, verarbeitet werden, muss die Schule die Schüler(innen) oder ihre Erziehungsberechtigten um Erlaubnis fragen. Das nennt sich im Datenschutz Einwilligung. Die Einwilligungserklärung muss zweckbezogen sein, also beschreiben, wozu die Daten genutzt werden sollen. Umfasst eine Einwilligungserklärung mehrere Zwecke, muss eine Wahlmöglichkeit (ja/nein) gegeben sein. Außerdem muss die Erklärung einen Hinweis auf das Widerrufsrecht enthalten. Die Einwilligung kann jederzeit ohne Begründung widerrufen werden.

Nach Artikel 8 Absatz 1 der DSGVO dürfen Schüler(innen) erst ab 16 Jahren wirksam in die Verarbeitung ihrer personenbezogenen Daten durch Dienstanbieter der Informationsgesellschaft einwilligen. Die Regelung, ab welchem Alter Schülerinnen oder Schüler selbst die Einwilligung geben können, wird allerdings unterschiedlich ausgelegt. In Nordrhein-Westfalen wird z. B. der entsprechende Absatz im Schulgesetz so interpretiert, dass bereits mit 14 eine selbstständige Einwilligung möglich ist.

In diesem Altersbereich ist eine doppelte Einwilligung durch die Schülerinnen und Schüler sowie deren Eltern empfehlenswert. Sollen kommerzielle Dienste (auch werbefinanziert) mit personenbezogenen Daten an der Schule genutzt werden, ist eine selbstständige Einwilligung erst ab 16 Jahren rechtens. Mit Erreichen der Volljährigkeit üben alle Schülerinnen und Schüler ihr Recht selbst aus.

Aufgepasst: Die Einwilligungserklärung darf nicht mit anderen Bedingungen verknüpft werden. Eine Koppelung mit der Schulanmeldung ist z. B. nicht rechtens.

3. DIE ZWECKBINDUNG

Mit dem Grundsatz der Zweckbindung ist gemeint, dass nur solche Daten erhoben und verarbeitet werden dürfen, für die ein eindeutiger und legitimer Zweck verfolgt wird. Für die Schule sind diese Zwecke in den Landesschulgesetzen und -verordnungen definiert. Für alle weiteren Daten, die nicht unmittelbar für den Schulbetrieb notwendig sind, muss sich die Schule eine Einwilligung geben lassen. Hier greift das Recht auf informationelle Selbstbestimmung.

4. DIE DATENMINIMIERUNG

Unter dem Grundsatz der Datenminimierung versteht die DSGVO, dass personenbezogene Daten sparsam erhoben werden müssen. Das heißt, dass bei der Datenverarbeitung immer nur so wenige Daten wie möglich erfasst und verarbeitet werden müssen: also nur die Daten, die für den jeweiligen Zweck unbedingt notwendig sind.

5. DIE RICHTIGKEIT DER DATEN

Der Grundsatz der Richtigkeit der Daten meint, dass die Daten aktuell und auf dem neusten Stand sein müssen. Unrichtige und nicht aktuelle Daten müssen gelöscht bzw. korrigiert werden. Dafür ist die Schule verantwortlich.

6. DIE MINIMIERUNG DER SPEICHERZEIT/ LÖSCHFRISTEN

Mit dem Grundsatz der zeitlichen Minimierung ist gemeint, dass Daten nur so lange wie notwendig vorgehalten werden. Die Notwendigkeit definiert sich aus dem jeweiligen Zweck. Die Regeln dafür ergeben sich aus den Landesschulgesetzen oder allgemeinen gesetzlichen Aufbewahrungsfristen. So gilt z. B., dass Zeugnisse bis zu 45 Jahre nach ihrer Ausfertigung noch erstellt werden können.

Chatverläufe und andere Kommunikationsdaten müssen hingegen zeitnah gelöscht werden. Der Datenschutz sieht Löschkonzepte vor, in denen spezifische Löschfristen festzulegen sind. Schulplattformen wie IServ bieten den Schulen vorkonfigurierte Löschkonzepte, auf die Schulen zurückgreifen können. Die fristgerechte Löschung kann dann voll automatisiert erfolgen. Selbstverständlich gilt für Daten jenseits der gesetzlichen Aufbewahrungspflichten das Recht auf informationelle Selbstbestimmung: Diese Daten löschen zu lassen ist jederzeit möglich und ein Grundrecht.

7. DIE INTEGRITÄT UND VERTRAULICHKEIT

Der Grundsatz der Integrität und Vertraulichkeit beinhaltet einerseits, dass die personenbezogenen Daten nicht unbemerkt verändert werden können, also integer bleiben, und andererseits, dass nur Berechtigte auf die Daten zugreifen können. Für beide Punkte muss die Schule technische Verfahren festlegen und dokumentieren.

8. DIE RECHENSCHAFTSPFLICHT

Unter der Rechenschaftspflicht wird verstanden, dass die für den Datenschutz verantwortliche Person – also die Schulleitung – nachweisen muss, was sie konkret für die Einhaltung des Datenschutzes getan hat. Dazu gehören die Dokumentationspflichten wie z. B. das Verzeichnis der Verarbeitungstätigkeiten, aber auch der Nachweis von Schulungsmaßnahmen.

BRAUCHT MEINE SCHULE EINE/EINEN DATENSCHUTZ-BEAUFTRAGTE(N)?

Jede öffentliche Schule muss eine/einen schulischen Datenschutzbeauftragte(n) (DSB) schriftlich unter Einbeziehung des Personalrats benennen. Die Daten der/des DSB sind der Landesdatenschutzbehörde zu melden. Auf der Website der Schule ist eine Kontaktmöglichkeit vorzusehen. Mehrere Schulen können unter Berücksichtigung ihrer Organisationsstruktur und Größe gemeinsam eine/einen DSB benennen. Das bietet sich insbesondere für kleinere Schulen wie z. B. Grundschulen an.

Die/der DSB kann auch ein externer Dienstleister oder eine externe Dienstleisterin sein. Bei der heutigen Belastung im Schulalltag bietet sich diese Lösung an. Nachteilig ist aber, dass eine/ein externer DSB nicht direkt am Schulleben teilnimmt. Die fachliche Qualifikation der/des DSB sollte neben der Kenntnis der Datenschutzrechte auch die Datenschutzpraxis an Schulen umfassen. Wissen im Bereich IT und Organisation sollten eine weitere Voraussetzung für die Benennung sein.

Die/der DSB darf nicht gleichzeitig der Schulleitung angehören oder IT-Admin der Schule sein, da ggf. Interessenkonflikte entstehen könnten. Die Zuständigkeit der/des DSB umfasst folgende Bereiche:

- die Beratung und Information der Schule in allen datenschutzrechtlichen Angelegenheiten einschließlich der Datenschutzfolgeabschätzung;
- die Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften;
- die Schulung und Sensibilisierung der an der Schule mit Datenverarbeitungsvorgängen betrauten Personen einschließlich der externen Auftragsverarbeiter(innen) sowie
- die Zusammenarbeit mit den Aufsichtsbehörden.

Bei der Beschaffung neuer Software-Produkte, mit denen personenbezogene Daten verarbeitet werden, ist die/der DSB immer mit einzubeziehen. Alle am schulischen Prozess Beteiligten, also Schülerinnen und Schüler, Eltern und Lehrkräfte, können die/den DSB jederzeit zu allen Fragen des Datenschutzes zu Rate ziehen. Die/der DSB ist bei der Erfüllung der Aufgaben hinsichtlich des Datenschutzes keinerlei Weisungen unterworfen. Geht es um die technische Sicherheit von Gebäudeinfrastruktur oder die IT, ist die/der DSB des Schulträgers einzubeziehen.

Digitalisierung ohne Cyber-Sicherheit ist wie Fahrradfahren ohne Helm. Das kann gut gehen, aber wenn es kracht, tut es weh.«

Quelle: bsi.bund.de/DE/Service-navi/Presse/Pressemitteilungen/Presse2019/BSI_im_Dialog_281119.html

WO WIRD DIE SCHULISCHE IT-SICHERHEIT GEREGELT?

Neben dem Konzept für die Verarbeitung der personenbezogenen Daten ist die Schule auch für den technischen und organisatorischen Schutz verantwortlich. Die entsprechenden Maßnahmen müssen nachweisbar und verschriftlicht sein. Sie bauen im Einzelnen aufeinander auf:

1. ZUTRITTSKONTROLLE

An erster Stelle steht die Zutrittskontrolle. Mit ihr soll verhindert werden, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen haben. Wie werden das Schulgebäude und die Server-Räume gesichert? Wer verfügt über Zutrittsmöglichkeiten?

2. ZUGANGSKONTROLLE

Mit der Zugangskontrolle sind Regelungen gemeint, die dafür sorgen, dass nur Befugte die personenbezogenen Daten nutzen können, also z. B. Berechtigungskonzepte mit Passwort oder biometrische Verfahren.

3. WEITERGABEKONTROLLE

Mit der Kontrolle der Weitergabe soll gewährleistet werden, dass die Daten durch Unbefugte weder kopiert, gelesen, verändert noch gelöscht werden können. Mögliche Maßnahmen sind z. B. die Verschlüsselung der Daten und die Protokollierung von Änderungen.

4. EINGABEKONTROLLE

Mit der Eingabekontrolle soll überprüft werden, wer Daten überhaupt eingeben, verändern oder löschen darf. Maßnahmen sind z. B. die Protokollierung und die Benutzeridentifikation.

5. AUFTRAGSKONTROLLE

Diese Kontrolle überprüft, ob die Auftragsverarbeitung durch Dritte gemäß den Weisungen der Auftraggeberin oder des Auftraggebers verarbeitet werden, z. B. durch die Festlegung von Weisungsbefugnissen oder Stichproben.

6. VERFÜGBARKEITSKONTROLLE

Mit dieser Kontrolle sollen Daten gegen Zerstörung und Verlust geschützt werden. Klimaanlagen, Virenschutz- und Backupkonzepte sind z. B. passende Maßnahmen.

7. TRENNUNGSGEBOT

Personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, müssen getrennt verarbeitet werden. Mögliche Maßnahmen sind z. B. getrennte Datenbanken oder getrennte Ordnerstrukturen.

Alle diese Maßnahmen nennt die DSGVO »technische und/oder organisatorische Maßnahmen« oder einfach kurz TOM. Mit den TOM soll unbefugter und unrechtmäßiger Zugriff auf die Daten verhindert werden. Die in den TOM festgelegten Maßnahmen beziehen sich nicht nur auf die Räume und Server in der Schule. Auch für an der Schule eingesetzte USB-Sticks mit personenbezogenen Daten sind Schutzmaßnahmen festzulegen. Gleiches gilt für externe Anbieter(innen) und Cloud-Dienste, die ebenso in die TOM mit einbezogen werden müssen.

Mit Blick auf die Datensicherung bzw. einen Backup-Plan bietet die DSGVO Interpretationsspielraum. Empfehlenswert ist auf jeden Fall ein IT-Sicherheitskonzept, das Backup-Pläne enthält und damit dem Anspruch der Verfügbarkeitskontrolle genügt. Die Einsatzbereitschaft ausgefallener Systeme sollte so schnell wie möglich wieder hergestellt werden können.

WELCHE REGELUNGEN GELTEN FÜR DIE WEBSITE DER SCHULE?

Verfügt die Schule über eine eigene Website, ist diese nicht nur die Visitenkarte der Schule in der Öffentlichkeit. Sie erfüllt auch viele kommunikative Aufgaben, die in aller Regel im Laufe der Zeit anwachsen. Werden auf der Website personenbezogene Daten erhoben, gelten natürlich auch hier die Regeln der DSGVO. Sollen Daten über Kontaktformulare erhoben werden, muss auf eine Datenschutzerklärung verwiesen werden. In dieser Erklärung muss erläutert werden, wo und zu welchem Zweck die Daten erhoben werden, wie die Verarbeitung erfolgt, wie lange und wo die Daten gespeichert und gelöscht werden. Außerdem muss eine Kontaktmöglichkeit zur/zum Datenschutzbeauftragten gegeben sein.

Wird eine Analyse- oder Tracking-Software eingesetzt, muss der Grund der Nutzung beim Aufruf der Website genannt werden und bei den Besucher(inne)n eine Abfrage erfolgen, ob und in welchem Umfang eine Erhebung der Nutzung erfolgen darf. Wichtig ist auch ein rechtssicheres Impressum der Website, das Auskunft über die Schule, die für die Website Verantwortliche oder den Verantwortlichen sowie die Macher(innen) der Website gibt. Sollen Fotos oder Videos von Schülerinnen und Schülern oder Lehrkräften veröffentlicht werden, wird eine Einverständniserklärung benötigt.

REGELUNGEN ZUR NUTZUNG PRIVATER GERÄTE

An den meisten Schulen gehört der Einsatz privater Geräte durch Lehrkräfte und/oder Schülerinnen und Schüler zum Alltag. Mittlerweile gibt es auch dazu Vorschriften und Regelungen durch die Bildungsministerien der Länder.

Grundsätzlich gilt, dass auf den privaten Geräten der Lehrkräfte keine dienstlichen personenbezogenen Daten gespeichert werden dürfen. In einigen Bundesländern dürfen die Schulleitungen es unter Auflagen erlauben.

Auch ist zu beachten, dass private Geräte in aller Regel technisch geringer geschützt sind als Dienstgeräte. Mit Schadsoftware können die Geräte ausgelesen werden. Mit den bekannten Antiviren-Programmen kann das Risiko zwar minimiert, aber nicht vollständig beseitigt werden.

IServ Akademie

VON BEGINN AN VON PROFIS LERNEN

Die Fortbildungsangebote der IServ-Akademie

BASISWISSEN, TIEFERES VERSTÄNDNIS ODER INDIVIDUELLE FRAGEN:

Unsere Fortbildungen begleiten Sie von Ihren ersten Schritten bis zum Expertenstatus. Lernen Sie die IServ Schulplattform in unseren Grundlagenschulungen kennen – oder vertiefen Sie Ihr Wissen in unseren Themen-Workshops oder individuellen Workshops. Immer gemeinsam mit echten IServ-Profis.

Mehr Infos unter: **iserv-akademie.de/schulungen**

Weitere Informationen zu unserer IServ Schulplattform finden Sie unter **iserv.de**

Bei Fragen oder für ein persönliches Beratungsgespräch wenden Sie sich bitte an:

T: +49 531 38821–02
E: vertrieb@iserv.de

IServ GmbH
Vossenkamp 6
38104 Braunschweig

T: +49 0531 38821–02
E: vertrieb@iserv.de
iserv.de

Geschäftsführer:
Benjamin Heindl,
Martin Hüppe, Jörg Ludwig

Stand: **Mai 2022**