Tipps & Antworten für die Praxis

Können die in **Teil B - Datensicherheit** geforderten Maßnahmen "*für eine datenschutzsichere Verarbeitung von personenbezogenen Daten*" auf den verschiedenen Betriebssystemen eingehalten werden? Gibt es Ausnahmen? Was muss ich tun? Die am Genehmigungsvordruck orientierte Tabelle gibt einen Überblick.

Darunter finden sich noch häufig gestellte Fragen in diesem Zusammenhang - **FAQ**

	Windows	OS X	Linux	iOS	Android
1. Vertraulichkeit					
Um sicherzustellen, dass nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können, setze ich folgende Maßnahmen um:					
Zugriffsschutz der eingesetzten privaten Endgeräte durch ein adäquates Verfahren (z. B. ein ausreichend sicheres Passwort)	Vor allem bei Geräten, die regelmäßig mit in die Schule genommen werden, sollte der Zugriffsschutz von Zeit zu Zeit geändert werden, z.B. durch Wechsel des Passwortes. Außerdem sollte darauf geachtet werden, dass Schüler die Anmeldung am Gerät nicht beobachten können, um das Passwort oder Sperrmuster zu merken. Ein Passwort sollte auch nicht irgendwo notiert sein, etwa im Deckel des Lehrerplaners, der dann vielleicht offen in der Klasse liegt.				
	Standard für den Zugriffsschutz ist noch immer das Passwort. Wichtig ist, dass die Anmeldung mit Zugriffsschutz zunächst aktiviert wird. Je nach Gerät gibt es zusätzlich zum Passwort weitere Anmeldeverfahren. Das können biometrische Verfahren wie der Fingerabdruck sein, eine PIN oder ein Security Key. Letztere sind meist auf aktuellere Geräte beschränkt. Das Passwort bleibt für die meisten Nutzer das gängigste Verfahren, den Zugriff auf das Gerät zu sichern. Zum Erstellen eines sicheren Passworts gibt es Informationen beim BSI[1]. Das Passwort wird beim Anlegen des dienstlichen Benutzers festgelegt. Gerade bei Geräten, die auch im Unterricht genutzt werden, ist es sinnvoll, ein zweites Anmeldeverfahren einzurichten,			Neben dem Zugriffsschutz über ein Passwort verfügen aktuelle Mobilgeräte auch über biometrische Verfahren, wie Fingerabdruck, Retina Scan oder Gesichtserkennung. In einer schulischen Umgebung bietet der Fingerabdruck eine gute und verlässliche Sicherung, da er von Schülern nicht eingesehen werden kann. In der Regel wird zusätzlich zum biometrischen Verfahren ein zweites Verfahren eingerichtet, meist ein Passwort/ Pin.	

[1] "BSIFB - Passwörter - BSI für Bürger." https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html. Aufgerufen - 12 Nov. 2020.

	wenn möglich. Eine Anmeldung mit Fingerabdruck oder Security Key können Schüler nicht ausspähen.				
	Das Passwort lässt sich unter **Konten** ändern. Auf vielen Windows Rechnern kann zum zusätzlichen Schutz auch noch ein Boot Passwort eingerichtet werden. Von der Nutzung eines Pin-Codes zum schnelleren Login wird abgeraten.	Das Passwort kann unter **Sicherheit** und **Benutzer** (Anmeldepasswort) geändert werden. Neuere Apple Notebooks haben einen Fingerabdruck Sensor in der Tastatur integriert. Dieser kann zusätzlich zum Passwort verwendet werden.	Unter Kontodetails ist das Passwort veränderbar. Bei Linux Systemen auf X86 Hardware ist es möglich, den Zugriffsschutz durch das zusätzliche Einrichten eines Boot Passwortes zu erhöhen.	Bei Geräten, die noch kein Touch ID oder Face ID haben, sollte ein komplexer Code genutzt werden. Unter Code kann die Komplexität eingestellt werden. Nutzen Sie mindest einen sechsstelligen Code, besser eine Kombination aus Buchstaben und Zahlen.	Falls ein Sperrmuster genutzt werden soll, muss dieses ausreichend komplex sein. Da es eventuell anhand von Wischspuren auf dem Display erkannt werden kann, ist von diesem Verfahren eher abzuraten. Passwörter müssen ausreichend komplex sein[2].
	Zusätzlicher Schutz durch Zwei Faktor Authentifizierung mit einem Security Key (z.B. Yubico) möglich.[3]				
automatische Sperre der privaten Endgeräte nach maximal 15 Minuten Inaktivität	Bei Geräten, die im Unterricht genutzt werden, sollte die Zeit, nach welcher bei Inaktivität die Bildschirmsperre aktiviert wird, lieber kürzer eingestellt werden. Das BSI empfiehlt 5 Minuten.				
	Die Einstelloptionen hierfür finden sich unter Konten > Anmeldeoptionen >	Zunächst muss eingestellt werden, nach welcher Zeit der Inaktivität ein		Unter Einstellungen kann die Zeitdauer für die Aktivierung der Bildschirmsperre	Die Einstellungen können unter Einstellungen > Sicherheit angepasst

[2] "BSIFB - Passwörter - BSI für Bürger." https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html. Aufgerufen - 06 Nov. 2019.
[3] "YubiKey für Unternehmen | Yubico." https://www.yubico.com/de/. Aufgerufen - 6 Nov. 2019.

	‘Anmeldung erforderlich’ (Win 10); Bildschirmschoner und dort ‘Anmeldeseite bei Reaktivierung’ (Win 8)	Bildschirmschoner oder der Ruhezustand aktiviert wird (Energie sparen). Danach kann unter Sicherheit die Abfrage eines Passwortes eingestellt werden.		angepasst werden.[4]	werden.[5]
Anlegen eines eigenen Benutzerkontos für dienstliche Zwecke (sofern technisch möglich)	Legen Sie in der Benutzerverwaltung ein zweites Benutzerkonto mit eingeschränkten Rechten an. Anders als der Hauptbenutzer sollte dieser zweite Benutzer keine Administrationsrechte haben. In einigen Bundesländern wird als Alternative zum dienstlichen Nutzerprofil die Nutzung eines verschlüsselten USB Sticks[6] empfohlen. Alle personenbezogenen Daten aus der Schule werden nur auf diesem Stick gespeichert und so strikt von privaten Daten getrennt. **Wichtig**: ● Es sollte einen Backup USB Stick geben, der ebenfalls verschlüsselt ist & auf den der 1. Stick regelmäßig gesichert wird. ● Alternativ könnte man den USB Stick in ein Lehrerverzeichnis auf dem Laufwerk eines PC in der Schule sichern. ● Es muss sichergestellt sein, dass Inhalte des USB Sticks nicht automatisch über einen Cloud Dienst gesichert werden. ● Bei Nichtnutzung USB Stick vom Rechner trennen & sicher aufbewahren.			Das Anlegen eines zusätzlichen Benutzerkontos ist nicht möglich. Deshalb wird hier eine Ausnahme gemacht.	Ob ein zusätzliches Benutzerkonto eingerichtet werden kann, hängt vom jeweiligen Gerät bzw. Hersteller ab. Einige Tablets, zum Beispiel Samsung, erlauben die Einrichtung weiterer Benutzerkonten, auch mit geringeren Rechten.

[4] "Bildschirmsperre einrichten (iOS 10-13) - mobilsicher.de." 12 Nov. 2020, https://mobilsicher.de/schritt-fuer-schritt/bildschirmsperre-einrichten-ios-10. Aufgerufen - 08. Nov. 2019.
[5] "Bildschirmsperre einrichten (Android) - mobilsicher.de." https://mobilsicher.de/schritt-fuer-schritt/bildschirmsperre-einrichten. Aufgerufen - 08. Nov. 2019.
[6] "USB Sticks und Datensicherheit – datenschutz-schule.info." https://datenschutz-schule.info/themen/usb-sticks-und-datensicherheit/. Aufgerufen - 08. Nov. 2019.

	Der Benutzer sollte aus Sicherheitsgründen als lokaler Benutzer angelegt werden.[7]				
Verschlüsselung der gespeicherten Daten durch ein geeignetes Verfahren z. B. bei externen Datenträgern	Windows 10 kann die Festplatte mit BitLocker verschlüsseln. Auch bei Windows 8 und 8.1 gibt es die BitLocker-Verschlüs-selung. Auf manchen Rechnern geht es nicht, da dort ein erforderlicher Chip fehlt. Hier gibt es jedoch Alternativen, z.B. VeraCrypt[8] oder BoxCryptor[9]	Kann bei OS X durch Aktivierung von File Vault (System-einstellungen) erreicht werden.	Für Linux gibt es spezielle Verschlüsselungssyst eme für die komplette Festplatte, z.B. Linux Unified Key Setup (Luks). Es ist möglich, die Festplatte direkt bei der Erstinstallation zu verschlüsseln. Unter aktuellen KDE Versionen lassen sich mit Plasma-Vault [10] – Verschlüsselte Container einrichten. Auch VeraCrypt ist für Linux verfügbar.	iOS ist vom System aus verschlüsselt.	Android erlaubt unter den Sicherheits-einstellungen eine Verschlüsselung des gesamten Gerätes. Diese sollte genutzt werden. Einige Hersteller bieten zusätzliche Möglichkeiten, z.B. Samsung Knox.
Sofern LOGINEO NRW eingesetzt wird	Zu empfehlen ist hier, dass die Zugangsdaten nicht im Browser gespeichert, sondern von Hand eingegeben werden, um einem Missbrauch des Login vorzubeugen. Alternativ könnte ein sicherer Passwortmanager genutzt werden.				

[7] "Erstellen eines lokalen Benutzer- oder Administratorkontos in ...." 4 Sep. 2019, https://support.microsoft.com/de-at/help/4026923/windows-10-create-a-local-user-or-administrator-account. Aufgerufen 9 Nov. 2019.
[8] "Downloads - VeraCrypt - Free Open source ...." 12 Nov. 2020, https://www.veracrypt.fr/en/Downloads.html. Aufgerufen - 08. Nov. 2019.
VeraCrypt - deutsch bei Heise unter https://www.heise.de/download/product/veracrypt-95747 Aufgerufen - 08. Nov. 2019.
[9] "Boxcryptor: Dateien in der Cloud sicher verschlüsseln." https://www.boxcryptor.com/de/. Aufgerufen - 08. Nov. 2019.
[10] "Plasma-vault Download (APK, DEB, EOPKG, RPM ... - pkgs.org." https://pkgs.org/download/plasma-vault. Aufgerufen 12 Nov. 2020.

und erreichbar ist: Bearbeitung und Speicherung von Dokumenten, die sensible personenbezogene Daten (z. B. Wortzeugnisse) enthalten, ausschließlich über den Online-Editor von LOGINEO NRW	Vorbereitete, anonym gehaltene Texte für Beurteilungen, Wortzeugnisse und ähnlich können aus einer Textverarbeitung in den Online-Editor kopiert werden.				
2. Integrität					
Damit die Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben, gewährleiste ich den Einsatz folgender Systeme:					
Einsatz eines (Betriebs-)Systems, für das aktuelle Sicherheitsupdates verfügbar sind	Bei Windows 10 ist alles O. K. für die kommenden Jahre. Der Support von Windows 8.1 wird Anfang 2023 enden. Ältere Versionen wie XP oder Vista gehen definitiv nicht mehr. Windows 7.1 wird seit Anfang 2020 nicht mehr unterstützt.	Für OS X gibt es bisher jedes Jahr eine neue Version des Betriebssystems (seit 11/2020 macOS Big Sur 10.16). Regelmäßige Sicherheitsupdates werden in der Regel nur für das aktuelle System und die beiden Vorgängerversionen bereitgestellt.[11] Wer	Verbreitete Linux Distributionen wie Ubuntu, Kubuntu usw. werden beständig aktualisiert. Es ist dabei nicht erforderlich, die tagesaktuellste Version zu nutzen. Eine LTS Version (Long Term Support) reicht, da es für diese 5 Jahre lang	Apple unterstützt auch ältere Mobilgeräte noch recht lange durch aktuelle Sicherheitsupdates. Sobald diese ausbleiben, ist es Zeit, das Gerät zu wechseln.	Android Geräte werden in der Regel nicht länger als zwei Jahre durch aktuelle Sicherheitsupdates unterstützt. Bei manchen Herstellern ist diese Frist sogar noch kürzer. Danach sollte das Gerät gewechselt werden. Google sagt für eigene Geräte (Pixel Smartphones)

[11] "Apple-Sicherheitsupdates - Apple Support." https://support.apple.com/de-de/HT201222. Aufgerufen - 08. Nov. 2019.

	Automatische Updates sollten einschaltet und gelegentlich manuell überprüft werden.	2019 noch auf OS X Yosemite 10.10.5 setzt, sollte auf eine neuere Version wechseln.	ausreichend aktuelle Sicherheitsupdates gibt.		Sicherheitsupdates für 3 Jahre zu.
Einsatz aktueller Virenschutz-Software	Microsoft Defender ist sehr gut, muss aber aktuell sein. Um die Vorgabe der Genehmigung zu erfüllen, sollte die Virenschutz-Software eines namhaften Herstellers als zusätzlicher Schutz installiert werden. Wer die Sicherheit optimieren möchte, installiert ein komplettes Sicherheitspaket.	Aktuell heißt es beim BSI “Bei Bedarf, etwa wenn ein Macs in einem heterogenen Netz betrieben wird, SOLLTEN neben den integrierten Schutzmechanismen von macOS zusätzlich Virenschutz-Lösungen von Drittanbietern eingesetzt werden.”[12] Mit Virenschutz ist man auf jeden Fall sicherer und schützt auch andere. Empfehlungen für Virenschutzsoftware [13]	Linux kommt ohne Virenscanner aus, da diese nur auf Windows Viren prüfen. Ein Virenscanner jedoch unverzichtbar, wenn Wine genutzt wird. Außerdem kann so die Weitergabe von Viren an Windows Systeme verhindert werden.	Ist die Installation einer Firewall oder eines Virenschutzprogramms nur durch Entfernen bzw. Unterwandern anderer durch das eingesetzte System vorgehaltener Sicherheitsmaßnahmen möglich (z.B. durch Rooten oder Jailbreak) oder der Nutzen für einzelne Geräte oder Systeme zweifelhaft und aus diesem Grund nicht zu empfehlen, so kann der Einsatz dieser Schutzmaßnahmen auf dem betreffenden Gerät unterbleiben. Eine solche Ausnahme sollte durch eine Anlage zur Genehmigung kurz dokumentiert und begründet werden.[14]	

[12] "SYS: IT-Systeme - SYS.2.4 Clients unter macOS - BSI." https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_4_Clients_unter_macOS.html. Aufgerufen 12 Nov. 2020.
[13] "10 Antivirus-Lösungen für Macs im Vergleich - Macwelt." 14 Jun. 2019, https://www.macwelt.de/a/12-antivirus-loesungen-fuer-mac-im-vergleich,3035954. Aufgerufen 9 Nov. 2019.
[14] "Sicherheits-Apps für Android-Geräte - mobilsicher.de." 25 Aug. 2015, https://mobilsicher.de/hintergrund/sicherheitsapps-fuer-android-geraete. Aufgerufen - 08. Nov. 2019.

Einsatz einer Firewall	Die Firewall von Windows muss aktiviert sein.	OS X bietet unter den Systemeinstellungen unter Sicherheit eine Firewall, die aktiviert sein sollte.	In der Standardinstallation ist in Linux keine Firewall aktiviert. Sie ist jedoch im System angelegt (UncomplicatedFire-wall).		Wer trotzdem eine Firewall haben möchte, kann dafür NetGuard oder NoRoot-Firewall nutzen, die ohne Rooten installiert werden können.[15]
3. Verfügbarkeit					
Damit die Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können, ergreife ich folgende Maßnahmen:					
regelmäßige Aktualisierung der (Betriebs-)Systeme	Nach Möglichkeit der Hardware sollte das System auf die aktuellste Version, Windows 10, aktualisiert werden, da diese die sicherste Version ist. Windows prüft standardmäßig auf Systemupdates. Größere Updates müssen zum Teil vom Nutzer gestartet werden und erfordern einen Neustart des	OS X macht in der Standardeinstellung regelmäßig auf Sicherheitsupdates und größere Versionsupdates aufmerksam. Diese sollten zeitnah vorgenommen werden. Ältere Geräte, die keine neuen Systemversionen mehr nehmen, können noch verwendet werden,	Für gängige Linux Distributionen erscheinen regelmäßige Updates der Betriebssysteme. Eine Aktualisierung von einer LTS Version zur nächsten ist ausreichend. Neuere Versionen bieten auch bei Linux oft Verbesserungen in der Sicherheits-architektur des Systems.	Apple unterstützt auch ältere Geräte in der Regel über mehrere Jahre mit aktuellen Versionen von iOS. Sind diese nicht mehr verfügbar und es gibt auch keine Sicherheits-updates mehr, sollte das Gerät gewechselt werden. iOS prüft regelmäßig auf Systemupdates und zeigt diese an. Die Installation muss	Bei vielen Android Geräten gibt es für einige Zeit regelmäßige Aktualisierung des Betriebssystems. Mehr als ein großes System-Update gibt es in der Regel jedoch nicht. Sobald das Gerät auch nicht mehr durch aktuelle Sicherheitsupdates unterstützt wird, sollte das Gerät gewechselt werden.

[15] https://mobilsicher.de/ratgeber/in-der-praxis-firewalls-fuer-das-smartphone.(Beitrag ist schon von 2016) Aufgerufen - 08. Nov. 2019.

	Systems.	solange Apple für die genutzte Version Sicherheitsupdates zur Verfügung stellt. Bei älteren Version müssen Updates manuell gestartet werden, neuere Versionen lassen auch automatische Updates zu.		vom Benutzer gestartet werden.	Systemupdates werden von Android angezeigt und müssen vom Benutzer gestartet werden.
regelmäßige Aktualisierung eingesetzter Anwendungen (z. B. Virendefinitionen)	Sicherheitsupdates sollten auf Automatik gestellt sein. Auch Office Anwendungen sollten möglichst aktuell sein. Es muss nicht das neueste Office Paket sein, doch eine 10 Jahre alte Office Suite kann ein Sicherheitsrisiko sein. Bei freien Office Paketen wie z.B. Libre Office sollte immer die neueste Version genutzt und diese regelmäßig aktualisiert werden.	Unter OS X werden Updates zu Anwendungen (über den App Store) vom System angezeigt und sollten regelmäßig durchgeführt werden. Nicht über den App Store erworbene Programme prüfen in der Regel eigenständig auf Updates. Wo dieses nicht der Fall ist, muss man selbst nachschauen.	Unter Linux empfiehlt es sich, vor allem auf Anwendungen mit einer größeren Entwickler Community zu setzen, da hier regelmäßige Updates gesichert sind. Gängige Linux Distributionen prüfen eigenständig auf Updates installierter Programme.	Der App Store auf iOS prüft regelmäßig auf Updates zu installierten Apps. Verfügbare Updates werden in der Standardeinstellung automatisch heruntergeladen und angezeigt, benötigen aber zur Installation den Benutzer. Ab iOS 12 gibt es eine Option für automatische Update Installation. Diese muss jedoch vom Nutzer aktiviert werden.	Gängige Android Systeme prüfen über den Google Play Store regelmäßig, ob Updates für installierte Apps verfügbar sind. Diese sollten auch installiert werden. Auch wenn Android Updates automatisch installieren kann, ist es gelegentlich erforderlich bei Updates eine Zustimmung zu geben, bevor diese installiert werden.
regelmäßige Backups der	Es empfiehlt sich eine Sicherung auf	Von Hause aus bietet Apple Time Machine	Linux bietet verschiedene Backup	iOS erlaubt es Daten über iTunes auf	Android Geräte erlauben es, Daten

verarbeiteten Daten	externe Festplatte (oder USB Stick) über ein Backup Programm. Die Festplatte sollte verschlüsselt sein und möglichst sicher aufbewahrt werden.	als regelmäßige Sicherung des kompletten Rechners an. In den Einstellungen von Time Machine sollte die Verschlüsselung der Backups aktiviert werden, da diese standardmäßig nicht eingeschaltet ist[16]. Alternativ können die verarbeiteten Daten in Logineo NRW oder einem anderen, sicheren von der Schule zur Verfügung gestellten Cloud Speicher gesichert werden.	Programme, die eine regelmäßige Sicherung auf eine Speichermedium erlauben (z.B. Gnome Disk Utility, Clonezilla). Alternativ ist es möglich, das komplette Home Verzeichnis /home manuell auf ein externes Speichermedium zu sichern.	einen Rechner zu sichern. Über die iTunes-Dateifreigabe können die Daten auch auf ein externes Laufwerk kopiert werden. Siehe dazu auch den Ratgeber “Variante 2: Backup auf lokalem Rechner” auf mobilsicher.de[17] Alternativ können wichtige Dateien über ein entsprechendes App manuell auf externe Laufwerke gesichert werden, z.B. DS file für Synology NAS. Ab OS X Catalina (10.15) übernimmt der Finder die Backup Funktionen von iTunes. Es ist außerdem möglich Daten auf einen (unverschlüsselten**!**) USB Stick zu sichern.	über Kabel auf einen Rechner zu übertragen. Je nach Betriebssystem des Rechners und Hersteller des Android Gerätes können dafür spezielle Programme erforderlich sein, z.B. Samsung Kies oder Dateiübertragung für Android. Bei Geräte, die eine Speicherkarte aufnehmen können, ist auch die Sicherung über eine solche Karte möglich, die dann außerhalb des Gerätes sicher aufbewahrt wird.[18]

[16] "Anpassen der Konfigurationseinstellungen für Time Machine ...." https://support.apple.com/de-de/guide/mac-help/cpmh0053/mac. Aufgerufen 9 Nov. 2019.
[17] "iOS: Daten-Backup leicht gemacht - mobilsicher.de." https://mobilsicher.de/ratgeber/daten-backup-leicht-gemacht. Aufgerufen - 08. Nov. 2019.
[18] "Daten sichern mit Helium (Android) - mobilsicher.de." https://mobilsicher.de/ratgeber/daten-sichern-mit-helium-android. Aufgerufen - 08. Nov. 2019.

4. Weitere Vorgaben					
Backups der in Teil A genannten Daten in Cloudspeicherdienste sowie die Verarbeitung dieser Daten in cloudbasierten Anwendungen, zu denen zwischen Schulleiterin bzw. Schulleiter und Anbieter kein gültiges Vertragsverhältnis zur Verarbeitung personenbezogener Daten im Auftrag besteht, sind nicht zulässig.					
	• Die Nutzung einer Cloud-basierten Anwendung wie z.B. Microsoft Office 365 ist nur zulässig, wenn diese von der Schule offiziell für Verwaltungsaufgaben genutzt wird, es also ein gültiges Vertragsverhältnis zwischen Schulleitung und Anbieter zur Verarbeitung personenbezogener Daten gibt. • In vielen Schulen gibt es zwar Office 365 Lösungen für den pädagogischen Bereich, nicht jedoch für den Bereich Verwaltung. In solchen Fällen ist eine Nutzung für Lehrkräfte zur Verarbeitung personenbezogener Daten aus der Schule nicht zulässig. • Backup- und Synchronisierungsdienste wie z.B. DropBox dürfen im Zusammenhang mit der Verarbeitung von personenbezogenen schulischen Daten **nicht** genutzt werden.				
Darauf ist insbesondere bei Systembackups von mobilen Endgeräten zu achten und die betreffenden Daten zwingend bei solchen Backups auszuschließen.					
	Backups, ob automatisch oder manuell, über Office 365 oder Microsoft OneCloud sind nicht zulässig, außer es handelt sich um eine offizielle schulische Lösung für den Verwaltungsbereich, wie oben beschrieben. Die	Die Nutzung von iCloud für Backups und Synchronisation sollte für das dienstlichen Benutzerkonto deaktiviert werden. Ausnahmen für Teilbereiche wie Keychain sind für erfahrene Nutzer		Bei iCloud ist es möglich im Benutzerkonto unter iCloud auszuwählen, welche Apps iCloud nutzen. Apps, welche für die Verarbeitung von personenbezogenen schulischen Daten genutzt werden, müssen von der	Android bietet automatisierte Backups und Synchronisation von Daten über Google Drive an. Schulische Daten müssen davon ausgeschlossen werden.[22] Gleiches gilt für entsprechende Funktionen von

[22] "Google-Konto: Synchronisation deaktivieren (Android 8) - mobilsicher.de." https://mobilsicher.de/schritt-fuer-schritt/synchronisieren-mit-google-konto-ausschalten-android-8. Aufgerufen - 08. Nov. 2019.

	Backup Dienste von Microsoft Konten sollten für das dienstliche Benutzerkonto deaktiviert werden.	denkbar.[19]		iCloud ausgeschlossen werden.[20] Das gilt auch für Apps, die ihre Daten verschlüsseln (z.B. TeacherTool[21]).	Herstellern wie z.B. Samsung. Ist dieses über die Backup Einstellungen nicht möglich, muss das Backup deaktiviert werden oder das Gerät sollte nicht genutzt werden für die Verarbeitung schulischer Daten.
Bei Nutzung von Schnittstellen zu schulischer IT-Infrastruktur, die einen direkten Zugriff digitaler Endgeräte auf personenbezogene Daten aus der Schule erlauben (z. B. IMAP für E-Mail, CalDAV für Kalender, CardDAV für Adressdaten oder WebDAV für Dateimanagementsysteme), ist sicherzustellen, dass andere auf dem angebundenen Endgerät installierte Anwendungen keinen Zugriff auf diese Daten haben können. (Beispiel: Zugriff von WhatsApp auf das Adressbuch). Im Zweifelsfall ist von der Nutzung der jeweiligen Schnittstelle oder der Anwendung abzusehen.					
	● Grundsätzlich sollte bei E-Mail Anwendungen eine strikte Trennung von dienstlichen und privaten E-Mails erfolgen, sofern es auf dem System nicht möglich ist, einen separaten dienstlichen Nutzer einzurichten. Das ist auf vielen mobilen Systemen der Fall. ○ Eine Trennung lässt sich hier erreichen, wenn zwei verschiedene E-Mail Clients/ Apps genutzt werden. Auch Kontakte sollten auf diese Weise getrennt werden. ● Wichtig ist grundsätzlich, dass Programme bzw. Apps genutzt werden, die nicht in die Backup- oder Cloud Funktion des Betriebssystems oder eines anderen Anbieters eingebunden sind. ● Wo eine Trennung nicht möglich ist oder man den Zugriff anderer Anwendungen auf die schulischen Daten nicht verhindern kann, sollte besser über das Webinterface der Schule auf E-Mails, Kontakte und Termine zugegriffen werden.				

[19] "iCloud-Speicher verwalten - Apple Support." 7 Oct. 2019, https://support.apple.com/de-de/HT204247. Aufgerufen 9 Nov. 2019.
[20] "iCloud konfigurieren - mobilsicher.de." 6 Mar. 2018, https://mobilsicher.de/ratgeber/icloud-konfigurieren. Aufgerufen - 08. Nov. 2019.
[21] "Ein wichtiges Vorwort - TeacherTool." http://www.teachertool.de/informationen-zum-datenschutz.pdf. Aufgerufen - 08. Nov. 2019.

	● Auf die Nutzung von Programmen oder Apps, die auf Adressbücher zugreifen, z.B. WhatsApp[23], Facebook, Instagram, SnapChat usw. sollte im Verzeichnis eines dienstlichen Benutzers verzichtet werden. ● Die Sicherheit von E-Mails kann durch Nutzung von Verschlüsselung deutlich erhöht werden, was den Versand angeht, wie auch die Speicherung. Alle verschlüsselt gesendeten und empfangenen E-Mails werden auch verschlüsselt gespeichert und damit vor dem Zugriff durch andere Anwendungen zusätzlich gesichert.			
	Mozilla Thunderbird ist eine gute Alternative, die E-Mail, Adressbuch und Terminverwaltung bietet und nicht mit einem zusätzliche Cloud Dienst verbunden ist.	Neben Mozilla Thunderbird bieten sich bei Linux noch andere Alternativen, die entweder mit dem System kommen oder nachträglich installiert werden können.	Unter iOS ist es möglich, in den Einstellungen bei Datenschutz einzustellen, welche Apps auf Kontakte und Kalender Zugriff haben. Umgekehrt können das Kontakte und das Termine App daran gehindert werden, auf Kontaktinformationen und Termine in anderen Apps zuzugreifen. Unter iOS kann für die Verschlüsselung von E-Mails Canary Mail[24] genutzt werden.	Android Geräte kommen oft mit zwei E-Mail Clients, Kalendern und Adressbüchern. Die von Google sind verbieten sich von selbst. Je nach System können die vom Gerätehersteller integrierten Apps genutzt werden, solange die nicht in eine Cloud synchronisiert oder gesichert werden. Sonst installiert man alternative Apps, von denen es zahllose gibt. Eine gute E-Mail Alternative ist

[23] Mittlerweile gibt es Möglichkeiten, WhatsApp an Zugriffen auf Kontakte zu hindern. Diese Möglichkeit ist nur für erfahrene User eine Option. "WhatsApp: Zugriff auf Kontakte verhindern - so geht's - CHIP Praxistipps." 26 Sep. 2017, https://praxistipps.chip.de/whatsapp-zugriff-auf-kontakte-verhindern-so-gehts_93842. Aufgerufen - 1 Oct. 2018.
[24] "Canary Mail." https://canarymail.io/. Aufgerufen - 12 Nov. 2020.

				K9-Mail[25] [26]. In aktuellen Versionen von Android kann der Zugriff von Apps auf Kontakte manuell in den Berechtigungen des Apps deaktiviert werden.
Der Zugang zur schulischen Basis-IT-Infrastruktur LOGINEO NRW oder der Abruf personenbezogener Daten der Schule über ungeschützte Netzwerke, z. B. öffentliche Hotspots, ist untersagt.				
	Achtung, dieses Verbot gilt grundsätzlich! Das bedeutet, auch wenn ein VPN genutzt wird, ist es **nicht** zulässig, über ungeschützte Netzwerke auf Logineo NRW zuzugreifen oder personenbezogene Daten der Schule abzurufen.[27] Ungeschützte Netzwerke meint vor allem öffentliche WLAN Hotspots, die kostenfrei und unkontrolliert für jedermann zugänglich sind. In derartigen Netzwerken ist es häufig leicht möglich auf fremde Daten oder Geräte zuzugreifen.			

Siehe auch:

- **Android** Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_109.pdf?__blob=publicationFile&v=7
- Orientierungshilfe zur datenarmen Konfiguration von **Windows 10** https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf
- Basissicherung für **iOS-Geräte** https://mobilsicher.de/checkliste/basissicherung-fuer-ios-geraete

[25] "K-9 Mail – Android-Apps auf Google Play." https://play.google.com/store/apps/details?id=com.fsck.k9&hl=de. Aufgerufen - 08. Nov. 2019.
[26] "K-9 Mail: App einrichten und E-Mail-Konten verknüpfen - Mobilsicher." https://mobilsicher.de/schritt-fuer-schritt/mail-app-k-9-mail-einrichten-und-e-mail-konten-verknuepfen. Aufgerufen - 08. Nov. 2019.
[27] In der ursprünglichen Version der Genehmigung hieß es noch "*Der Zugang zur schulischen Basis-IT-Infrastruktur LOGINEO NRW oder der Abruf personenbezogener Daten der Schule über ungeschützte Netzwerke, z. B. öffentliche Hotspots,* ***ohne entsprechende Schutzmaßnahmen zu treffen****, ist untersagt.*" Der Passus "ohne entsprechende Schutzmaßnahmen zu treffen" wurde gestrichen.

- Backup bei Mobilgeräten (**iOS, Android**) https://mobilsicher.de/hintergrund/backup-smartphone-daten-sichern-2
- Mobilsicher.de - Das Infoportal für mehr Sicherheit auf **Smartphone** und **Tablet** https://mobilsicher.de/

Sicheres Löschen von Dateien und Verzeichnissen

Achtung! Löscht keine Dateien oder Verzeichnisse aus Backups

- **Windows** - **BleachBit** 2.0 for Windows XP, Vista, 7, 8, 8.1, and 10 (32-bit and 64-bit), mehrsprachige Version
- **Linux** - **BleachBit for Linux** (die Version wählen, welche zur eigenen Linux Version passt)
- **Apple** - unter OS X 10.04 - 10.10 kann man sicher löschen mit dem “Papierkorb sicher entleeren”. Ab OS X 10.11 gibt es diese Funktion nicht mehr, da Apple nicht weiterhin garantieren kann, dass dieses mit der anderen Architektur von SSD Festplatten funktioniert. Als Ausweg empfiehlt sich die Verschlüsselung der gesamten Festplatte.

Thema Verschlüsselung

- Für die Verschlüsselung externer Medien wie externer Festplatten (auch SSD), USB Sticks, SD Karten oder von Netzlaufwerken empfiehlt sich die Nutzung von speziellen Programmen zur Verschlüsselung. Der Vorteil ist, dass man je nach Software Betriebssystem übergreifend arbeiten kann. Das ist bei den Verschlüsselungsmechanismen der Betriebssysteme selbst oft nur eingeschränkt möglich.
  - **Boxcryptor**, ein deutscher Anbieter, man zahlt, was man möchte: Windows, OS X, Linux - https://www.boxcryptor.com/de/ (auch nutzbar unter Android und iOS)
  - **VeraCrypt**, aus Frankreich, kostenlos, Open Source; verfügbar für Windows, OS X, Linux; Download bei Heise - https://www.heise.de/download/product/veracrypt-95747

Thema 2 Faktor Authentifizierung

Was bedeutet 2 Faktor Authentifizierung?

- Mit 2 Faktor Authentifizierung (2FA) ist die Anmeldung an einer Plattform oder einem Endgerät mit zwei separaten Sicherheitsabfragen gemeint. Der Nutzer loggt sich zunächst mit seinem Benutzernamen und Kennwort ein und nutzt dann ein zweites Geheimnis, um den Login abzuschließen.

Was ist der Unterschied zu den oben genannten Möglichkeiten weitere Anmeldemöglichkeiten einzurichten?

- Wenn man alternative Anmeldemöglichkeiten einrichtet, wie etwa Passwort und Fingerabdruck, dann stellen diese gleichwertige alternativ nutzbare Möglichkeiten für den Benutzer dar, sich am Rechner oder Mobilgerät anzumelden. Der Fingerabdruck kann nicht verhindern, dass jemand sich über das Passwort Zugriff verschafft, wenn es ihm gelingt, dieses zu erraten.
- Bei 2FA gibt es zwei Abfragen, z.B. Passwort und einen Security Key oder Fingerabdruck und Security Key, die alle beide den Zugriff schützen. Ohne den zweiten Faktor, im Beispiel ein Security Key, ist ein Zugriff nicht möglich, auch wenn etwa das Passwort erraten wurde. Dadurch ist ein über 2FA geschützter Zugang deutlich sicherer vor unbefugten Zugriffen.

Wovon hängt es ab, ob 2FA genutzt werden kann?

- Ob 2FA unterstützt wird, hängt von verschiedene Faktoren ab.
    - Unterstützt die Anwendung/ App oder die Plattform das Verfahren?
    - Welches 2FA Format unterstützt die Anwendung/ App oder die Plattform? - Die Nutzung von Security Keys ist auf mobilen Betriebssystem deutlich eingeschränkter als auf Desktop OS.

FAQ

- An meiner Schule hat die Schulleitung bereits Genehmigungen für die Verarbeitung von schulischen Daten auf privaten Endgeräten an die Lehrkräfte erteilt. Brauche ich die neue Genehmigung?
    - Nein, nicht unbedingt. Die neuen Genehmigungsvordrucke sind laut der Dienstanweisung vom Februar 2018 verpflichtend für neu zu erteilende Genehmigungen. Nach einem Dienst Mail von Staatssekretär Richter vom 02.05.2018 können alte Genehmigungen jedoch weiter genutzt werden - "*Ausdrücklich darauf hinweisen möchte ich, dass in der Vergangenheit erteilte Genehmigungen weiterhin Bestand haben. Die Neufassung der DA ADV löst keinen neuen Handlungsdruck aus.*" Auch wenn die VO-DV I macht in §2 Abs. 2 Vorgaben macht, wie eine Genehmigung auszusehen hat, gibt das Dienst Mail Schulleitungen einen gewissen Spielraum in ihrer Entscheidung bezüglich der weiteren Nutzung bestehender Genehmigungen.

- Für welche persönlichen Daten gilt die Genehmigung?
    - Sie gilt für exakt die Daten, welche in der Genehmigung unter "Art der verarbeiteten Daten und Dokumente" aufgelistet sind, die für die es eine rechtliche Grundlage gibt (3.1 und 3.2) und die, welche nur mit einer Einwilligung verarbeitet werden dürfen (3.3).

- Wie sieht es mit anderen persönlichen Daten aus der Schule aus?
    - Sofern sie nicht unter die unter 3.1, 3.2, oder 3.3 gelisteten persönlichen Daten fallen, dürfen sie auf privaten Endgeräten von Lehrkräften grundsätzlich nicht verarbeitet werden. Für die unter 3.3 gelisteten Daten ist eine Einwilligung der Betroffenen

erforderlich. "*Die Liste kann an den Schulen ganz unterschiedlich sein und ist ggf. anzupassen*."[28] D.h. es könnten auch andere personenbezogene Daten mit Einwilligung der Betroffenen auf privaten Endgeräten von Lehrkräften verarbeitet werden.

- Was ist mit den Zeugnisnoten, die über das externe Notenmodul von SchiLD NRW eingegeben werden können und ähnliche Lösungen?
    - Auch hier gilt die Vorgabe der Dienstanweisung. Solange keine Genehmigung zur Verarbeitung von schulischen Daten auf ihrem privaten Endgerät von ihrer Schulleitung vorliegt, dürfen sie keine Noten über das externe Notenmodul auf ihrem Rechner eingeben. Zeugnisbemerkungen könnten sie jedoch auch ohne Genehmigung anonymisiert auf ihrem Rechner vorbereiten und dann in der Schule mittels USB Stick auf einen Verwaltungsrechner übertragen und in die Zeugniseingabe hineinkopieren.

- Gibt es Dinge, die ich überhaupt ohne Genehmigung auf einem privaten Endgerät verarbeiten darf?
    - Die gibt es wie zuvor. Unterrichtsvorbereitungen, Stundenentwürfe, Arbeitsmaterialien, Klassenarbeiten und Tests dürfen weiterhin ohne irgendeine Genehmigung auf privaten Geräten verarbeitet werden. Sie dürfen jedoch keine persönlichen Daten aus der Schule enthalten. D. h. möchte ich zum Beispiel Arbeitsmaterialien erstellen, welche die Namen von Schülerinnen und Schülern der Lerngruppe enthalten, so ginge dieses noch mit dem Vornamen alleine. Sobald der komplette Namen auftaucht, bewegt man sich schon in einem Grenzbereich.
    - In Stundenentwürfen dürfen dabei keine Schülernamen mit Anmerkungen zu Problemen oder Sozialverhalten auftauchen.

- Ich möchte die Genehmigung nicht unterzeichnen, da ich nicht sicher bin, ob ich die Vorgaben im "Teil B - Datensicherheit" einhalten kann. Gibt es trotzdem eine Möglichkeit, Daten aus der Schule auf meinem privaten Endgerät zu verarbeiten?
    - Nein. Hier gibt es leider keine Ausnahmen.
    - Aber es gibt durchaus Möglichkeiten, trotzdem etwas zu machen.
        - Förderempfehlungen, Wortzeugnisse, Beurteilungen, Gutachten, Anmerkungen zum Sozialverhalten, Mitteilungen und ähnliche können durchaus ohne Genehmigung auf einem privaten Endgerät **vorbereitet** werden, **wenn dabei auf die Nutzung jeglicher persönlicher Daten verzichtet wird**. Das bedeutet, man ersetzt Namen und andere persönliche Daten durch Platzhalter. Um die Texte hinterher zuordnen zu können, versieht man sie mit Nummern oder ähnlich, die

[28] "Handreichung zur Genehmigung - Medienberatung NRW." 27 Mar. 2018, Seite 6, https://www.medienberatung.schulministerium.nrw.de/Medienberatung-NRW/Datenschutz/Dokumente/Handreichung-zur-Genehmigung-der-Nutzung-privater-Endgera%CC%88te.pdf. Aufgerufen 9 Nov. 2019.

man über eine ausgedruckte Liste mit den Namen der Schülerinnen und Schüler abgleichen kann. Die Datei mit den Texten nimmt man hinterher mit in die Schule und ersetzt dort die Platzhalter durch die Namen entsprechend der Liste. Taucht zum Beispiel ein Vorname in einem Text mehrfach auf, kann man ihn in der Textverarbeitung leicht durchsuchen und ersetzen mehrfach einfügen.

- Selbiges funktioniert auch mit Notenlisten. Die Namen der Schülerinnen und Schüler ersetzt man auch hier durch einen Platzhalter. Das kann eine Nummer sein oder ein Fantasiename. Letzterer sollte jedoch nicht durch seine Gestaltung Rückschlüsse auf die echte Person zulassen. Die Nummern können sich durchaus an der Nummerierung der Klassenliste orientieren, die man ohne Genehmigung sowieso nicht auf dem Rechner gespeichert hat. Zur Sicherheit sollten auch die Namen der Lerngruppen abgeändert werden. Aus den Noten oder Anmerkungen dazu dürfen jedoch keine Rückschlüsse auf die Person möglich sein.

- Ich habe für mein Gerät eine Genehmigung der Schulleitung erhalten. Eine neue Version des Betriebssystems ist herausgekommen, doch mein Gerät erhält es nicht. Was soll ich tun?
  - Im **Teil B** unter **Nummer 3** heißt es, man sorgt für eine “regelmäßige Aktualisierung der (Betriebs-)Systeme”. Wenn dieses nicht möglich ist, besteht noch kein Grund zur Sorge, solange für diese Version weiterhin “aktuelle Sicherheitsupdates verfügbar” sind (siehe **Teil B Nummer 2**).
    - Je nach Hersteller können die Intervalle zwischen den aktuellen Sicherheitsupdates variieren. Gerade bei Android Geräten kann es schnell passieren, dass irgendwann aktuelle Sicherheitsupdates ausbleiben. Das ist vor allem der Fall bei kleineren Herstellern. Google veröffentlicht monatliche Sicherheitsupdates. Mehr als ein Vierteljahr sollte nicht vergehen zwischen den Sicherheitsupdates, wenn das Betriebssystem selbst nicht mehr aktualisiert wird auf die neueste Version.
  - Erst wenn es keine aktuellen Sicherheitsupdates mehr gibt, bleibt nur noch eines über, dieses Gerät aus der Liste der durch die Schulleitung genehmigten Geräte streichen zu lassen.

- Was genau meint **Anlegen eines eigenen Benutzerkontos für dienstliche Zwecke?**
  - Damit ist ein Benutzerkonto auf Ebene des Betriebssystems gemeint. Beim Anmelden am Betriebssystem des Rechners oder mobilen Endgerätes (Login) wählt man den Nutzer aus, mit welchem man sich anmelden möchte. Dieser Nutzer hat einen eigenen Desktop und einen eigenen Dateibereich sowie eigene Programme. Die Daten, welcher dieser Benutzer erzeugt, müssen auch in dessen Benutzerverzeichnis gespeichert werden, sodass sie für andere auf dem System eingerichtete Nutzer nicht sichtbar sind.

- Auf meinem Gerät kann ich keinen zweiten Benutzeraccount einrichten. Erhalte ich jetzt keine Genehmigung?
    - Das hängt vom jeweiligen Betriebssystem ab. In **Teil B Nummer 1** heißt es deswegen “Anlegen eines eigenen Benutzerkontos für dienstliche Zwecke (sofern technisch möglich).” Das bedeutet, wenn es technisch nicht möglich ist, muss kein zweites Benutzerkonto angelegt werden. Das ist zum Beispiel der Fall bei iOS Geräten. Bei vielen Android Geräten kann ebenfalls kein zweiter Benutzer angelegt werden. Hier sollte man sich jedoch schlau machen. Android Tablets von Samsung beispielsweise erlauben das Anlegen weiterer Benutzer. Wenn dieses möglich ist, **muss** davon Gebrauch gemacht werden.

- Hat die Schulleitung das Recht zu kontrollieren, ob ich mit meinem privaten Endgerät die Vorgaben der Genehmigung einhalte? Muss ich der Schulleitung dieses an meinem Gerät zeigen und vorführen?
    - In der VO DV I, §2 Ab 2 heißt es “*Die Lehrerinnen und Lehrer sind verpflichtet, der Schulleiterin oder dem Schulleiter alle **Auskünfte** zu erteilen, die für die datenschutzrechtliche Verantwortung erforderlich sind.*”
    - Diese Formulierung lässt einigen Spielraum. Vorstellbar ist damit auch, dass die Schulleitung sich die Einhaltung der datenschutzrechtlichen Vorgaben von ihnen vorführen lässt. Sie hat dabei jedoch nicht das Recht, ihre persönlichen Daten einzusehen. Von daher ist es zu empfehlen, auch bei Geräten bzw. Betriebssystemen, welche die Einrichtung eines zweiten Benutzers nicht zulassen, persönliche von schulischen Daten sauber zu trennen.
    - Sie sind ihrer Schulleitung gegenüber grundsätzlich immer zur Auskunft verpflichtet, wenn es um Fragen geht im Zusammenhang mit der erteilten Genehmigung.

- Worüber kann die Schulleitung Auskunft verlangen in Bezug auf die Verarbeitung schulischer Daten auf meinem genehmigten privaten Endgerät?
    - Die Schulleitung kann Auskunft darüber verlangen, ob die Vorgaben der Genehmigung eingehalten werden. Das bedeutet:
        - Die Art der verarbeiteten persönlichen Daten aus der Schule. Entsprechen sie den in 3.1, 3.2 oder 3.3 aufgeführten für eine Verarbeitung zugelassenen Daten? Verarbeiten sie also nur die Daten, welche für eine Verarbeitung auf privaten Endgeräten zugelassen sind und davon auch nur die, welche sie laut ihrer schulischen Funktion verarbeiten dürfen und solche, für welche eine Einwilligung der Betroffenen vorliegt?
        - Werden die in Teil B aufgeführten Maßnahmen “für eine datenschutzsichere Verarbeitung von personenbezogenen Daten” eingehalten?
        - Werden die Löschfristen eingehalten?

- In der VO-DV I § 2 (2) heißt es - “Die Genehmigung darf nur erteilt werden, wenn [...] ein angemessener technischer Zugangsschutz nachgewiesen wird.” Was bedeutet das?
    - Es bedeutet, dass die Genehmigung den Nachweis der in Teil B aufgeführten Maßnahmen “für eine datenschutzsichere Verarbeitung von personenbezogenen Daten” für das jeweilige Gerät voraussetzt, für welches die Genehmigung gegeben werden soll.

- Wer muss den “angemessenen technischen Zugangsschutz” nachweisen und wer beurteilt, ob der technische Zugangsschutz angemessen ist?
    - Den Nachweis muss die Lehrkraft erbringen, die eine Genehmigung für ein privates Gerät einholen möchte. Die Beurteilung, ob der von der Lehrkraft nachgewiesene technische Zugangsschutz angemessen ist, liegt bei der Schulleitung. Diese kann den schulischen Datenschutzbeauftragten bei der Beurteilung um Unterstützung bitten.

- Ich bin mir sicher, dass ich alle in Teil B aufgeführten Maßnahmen für eine datenschutzsichere Verarbeitung von personenbezogenen Daten erfüllen kann. Meine Schulleitung erteilt mir trotzdem keine Genehmigung. Darf sie das?
    - Sie darf dieses. Die Schulleitung trägt in Bezug auf die Einhaltung datenschutzrechtlicher Vorschriften für ihre Schule die Verantwortung. Aus diesem Grunde kann sie eine Genehmigung verweigern.
    - Wie viele Geräte bzw. welche Art von Endgerät eingesetzt werden dürfen, obliegt komplett der Entscheidung der Schulleitung.

- Was hat es mit der Vorabkontrolle gemäß § 10 Abs. 3 DSG NRW durch den zuständigen behördlichen Datenschutzbeauftragten auf sich?
    - Mit Beginn der Umsetzung der Datenschutz Grundverordnung (DS-GVO) ist diese Vorgabe obsolet geworden. Eine Vorabkontrolle durch den schulischen Datenschutzbeauftragten ist nicht mehr erforderlich.
    - Die Schulleitung kann den schulischen Datenschutzbeauftragten jedoch beratend hinzuziehen.
        - Dabei wird der Datenschutzbeauftragte auf die eingetragenen Geräte bezüglich des Betriebssystems schauen. Je nach Gerät ergeben sich dabei sehr schnell mögliche Problemfälle. Bei älteren Android Tablet- oder Smartphone Modellen ist klar, dass hier die unter **Teil B - Datensicherheit** vorgegebenen Maßnahmen nicht erfüllt werden können. Entsprechend wird die Anmerkung ausfallen.

    - Wo sich der schulische Datenschutzbeauftragten nicht sicher ist, wird er entweder entsprechende Anmerkungen machen oder um Klärung bitten, bevor er eine Unterschrift unter die Genehmigung setzt.
    - Werden unter **Teil B - Datensicherheit** Maßnahmen durchgestrichen oder abgeändert, wird dieses vom Datenschutzbeauftragten ganz sicher kritisch hinterfragt werden.

- Sind die Ratschläge, welche der Datenschutzbeauftragte der Schulleitung bezüglich ihrer Entscheidung ob eine Genehmigung erteilt werden sollte oder nicht, bindend?
    - Nein, die Ratschläge des Datenschutzbeauftragten haben keinen bindenden Charakter. Die Schulleitung als verantwortliche Person für den Datenschutz an der Schule trifft die Entscheidung unabhängig. Es ist jedoch davon auszugehen, dass die Mehrheit der Schulleitungen sich an den Empfehlungen der Datenschutzbeauftragten orientieren werden.

- Auf meinem privaten Endgerät, auf welchem ich schulische Daten mit Genehmigung durch die Schulleitung verarbeite, ist irgendetwas komisch. Was soll ich tun?
    - Wenn ein Verdacht besteht, dass die Sicherheit der verarbeiteten schulischen Daten nicht mehr gewährleistet ist und es möglicherweise zu einem Datenschutzvorfall gekommen ist**, muss** die Schulleitung **unmittelbar** informiert werden. Diese wird den Datenschutzbeauftragten informieren und man wird entscheiden, was zu tun ist. Im Falle eines tatsächlichen Datenschutzvorfalls, z.B. eines Diebstahls, muss die Schulleitung innerhalb von 72 Stunden nach Bekanntwerden die Aufsichtsbehörde informieren. Gegebenenfalls sind auch die betroffenen Personen zu informieren, um deren Daten es geht.

- Das private Endgerät, auf welchem schulische Daten mit Genehmigung der Schulleitung verarbeite, ist mir abhanden gekommen (verloren/gestohlen). Was ist zu tun?
    - Sie sind verpflichtet, die Schulleitung **umgehend** zu informieren, damit entsprechende Schritte zur Schadensbegrenzung eingeleitet werden können.

- Das private Gerät, auf welchem ich mit Genehmigung der Schulleitung schulische Daten verarbeite, ist defekt oder zu alt und ich möchte es ersetzen. Was muss ich tun?
    - Das alte Gerät sollte bei der Schulleitung “abgemeldet” werden und es wird aus der Genehmigung gestrichen. Für das neue Gerät braucht es selbstverständlich wieder eine Genehmigung. Ob dafür eine neue Genehmigung erstellt wird oder ob man das

neue Gerät lediglich in der bestehenden Genehmigung ergänzt, bleibt letztlich der Schulleitung überlassen. Am einfachsten wird es vermutlich sein, ein zusätzliches Formular auszufüllen für das neue Gerät.
    - Sorgen sie bitte außerdem dafür, dass alle schulischen Daten vom ausgemusterten Gerät gelöscht werden.
        - Sollte das Gerät nicht mehr reagieren und eine Datenlöschung nicht möglich sein, muss es zur Not zerstört werden.
        - Bei Rechnern kann unter Umständen die Festplatte ausgebaut und über einen anderen Rechner gelöscht werden. Im Zweifelsfall suchen sie sich Unterstützung bei Experten.
        - Eine Löschung muss unbedingt fachgerecht vorgenommen werden, da Daten sonst unter Umständen wiederherstellbar sind.
        - Eventuell ist es möglich, das Altgerät professionell über einen Entsorger des Schulträgers fachgerecht zerstören zu lassen.

- Ich habe zu Hause ein Computer, der nicht mit dem Internet verbunden ist und auf dem möchte ich nichts anderes tun als schulische Daten zu verarbeiten. Geht das?
    - Ein Computer, der nicht mit dem Internet verbunden ist, kann die in **Teil B - Datensicherheit** geforderten Maßnahmen in der Regel nicht einhalten. Auch wenn der Computer durch die Trennung vom Internet nicht direkt durch Zugriff von außen gefährdet ist, so können doch andere Gefahren drohen, die beispielsweise die Integrität oder Verfügbarkeit beeinträchtigen. Ein Virus könnte über einen USB Stick auf den Rechner gelangen und zur Vernichtung der Daten führen, da ohne Internet die Virendefinitionen der Antiviren Software mit großer Wahrscheinlichkeit total veraltet sein werden. Schulleitungen sollten für solche Rechner besser keine Genehmigung erteilen.

- Warum soll man auch die Seriennummer eines Gerätes angeben, für welches man eine Genehmigung beantragen möchte?
    - Im Falle einer Beschädigung eines Gerätes beim Einsatz in der Schule besteht ggf. Anspruch auf Entschädigung. Ohne die Genehmigung wird ein solcher Fall gar nicht erst geprüft.

- Wenn ich eine Genehmigung für die Verarbeitung schulischer Daten auf einem Smartphone oder Tablet von meiner Schulleitung erhalten habe, darf ich dann damit auch Fotos und Videos von Schülern für schulische Zwecke aufnehmen und verarbeiten?
    - Ja, das ist entsprechend der Genehmigung **Teil A - Art der verarbeiteten Daten und Dokumente, 3.3** möglich. Es **muss** dafür jedoch eine aktuelle und datenschutzkonforme Einwilligung der Betroffenen vorliegen. Je nach Art der Aufnahmen, sollte diese

Einwilligung anlassbezogen eingeholt werden. Die Einwilligung muss immer gegenüber der Schulleitung abgegeben werden, um rechtswirksam zu sein. Die Schulleitung sollte also zumindest in Kenntnis der Einwilligung sein.

- **Wichtig!** Gerade bei Smartphones und Tablets muss darauf geachtet werden, dass die Fotos und Videos, auf welchen Schülerinnen und Schüler zu sehen sind, nicht in eine Cloud gespeichert werden.
- Bei **Android** kann man dieses leicht verhindern, indem man ein weiteres Kamera App installiert. Sobald damit die ersten Aufnahmen gemacht wurden, fragt das System nach, ob die Fotos bzw. Videos in Google Fotos gesichert werden sollen. Das muss dann abgelehnt werden und die Fotos verbleiben alleine auf dem Gerät.
- Bei **iOS** muss die iCloud Speicherung entsprechend deaktiviert werden.

- Kann für ein Mobilgerät eine Genehmigung für die Verarbeitung schulischer Daten, wenn es gerootet (Android) ist oder einen Jailbreak installiert hat (iOS)?
  - Nein, bei Geräten, in deren Systemarchitektur dermaßen eingegriffen wurde, ist die Integrität des Betriebssystems und damit die Sicherheit nicht mehr gewährleistet. Eine Genehmigung kann für ein solches Gerät nicht erteilt werden.

- Kann ich auf meinem Android Tablet/ Smartphone für das ich eine Genehmigung für die Verarbeitung schulischer Daten erhalten habe, die Installation aus unsicheren Quellen einschalten?
  - Nein, das geht nicht, da es die Sicherheit des Gerätes gefährden kann. Nur für Apps, die aus dem Google Play Store ist sichergestellt, dass diese Anwendungen keine keinen Schadcode enthalten.

Allgemeine Fragen zur Genehmigung

- Meine Schule hat aktuell keine Schulleitung. Wer kann mir eine Genehmigung zur Verarbeitung von schulischen Daten auf meinem privaten Endgerät erteilen?
  - Hat eine Schule aktuell keine Schulleitung, kann die Genehmigung nur durch eine Person erteilt werden, welche die Schulleitung dauerhaft rechtlich vertritt. Das ist in der Regel eine kommissarische Schulleitung. Diese übernimmt die Aufgaben der Schulleitung und damit auch die datenschutzrechtliche Verantwortung (ADO §26).

- Die Schulleitung hat gewechselt. Ist meine Genehmigung zur Verarbeitung von schulischen Daten auf meinem privaten Endgerät, die mir von der vorherigen Schulleitung erteilt wurde, weiter gültig?
    - Ja, die Genehmigung behält nach den Regelungen des VwVfG ihre volle Gültigkeit und Wirksamkeit bei einem Wechsel der Schulleitung. (*Nach Auskunft des des - Referat 212 - Arbeits- und Gesundheitsschutz, Datenschutz, Informationsfreiheit*)

- Ich bin Lehramtsanwärter(in) und möchte mein privates Endgerät zur Verarbeitung von schulischen Daten einsetzen. Brauche ich eine Genehmigung? Muss ich diese Genehmigung bei der Schule oder beim ZfSL beantragen?
    - Ja, eine Genehmigung ist erforderlich. Sie muss bei der Schulleitung ihrer Ausbildungsschule beantragt werden, da nur diese die Genehmigung für die Verarbeitung personenbezogener Daten aus ihrer Schule erteilen kann.

- Ich bin Schulsozialpädagoge/ Schulsozialarbeiter. Kann ich mit Genehmigungsformular eine Genehmigung zur Verarbeitung von schulischen Daten auf meinem privaten Endgerät bei der Schulleitung beantragen?
    - Nein, das geht nicht, denn diese Genehmigung ist nur für Lehrkräfte gedacht. Für andere Personen als Lehrkräfte und die Schulleitung selbst sieht das Schulgesetz NRW keine Genehmigung zur Verarbeitung von schulischen Daten auf einem privaten Endgerät vor. Darüber hinaus fallen viele der Texte, die im Rahmen ihrer Tätigkeit entstehen, wie z.B. Fördergutachten nicht unter schulische Daten, deren Verarbeitung auf privaten Endgeräten zulässig ist.

- Ich bin als Lehrkraft an zwei Schulen tätig (Förderpädagoge oder Teilabordnung). Reicht eine Genehmigung zur Verarbeitung von schulischen Daten auf meinem privaten Endgerät?
    - Nein, sie müssen von den Schulleitungen beider Schulen eine Genehmigung einholen, um die schulischen Daten der von ihnen unterrichteten Schüler an beiden Schulen auf ihrem privaten Endgerät verarbeiten zu können.

- Ich bilde an meiner Schule Lehramtsanwärter aus. Muss ich eine Genehmigung haben, wenn ich Beurteilungen für diese schreibe? Falls ja, wer erteilt sie mir?
    - Eine Genehmigung ist erforderlich. Anders als das Genehmigungsformular aktuell (Stand November 2019) angibt, muss diese jedoch nach einer Information des MSB beim Schulleiter eingeholt werden (und **nicht** beim Leiter des ZfSL). Entsprechende Änderungen der Genehmigung und VO-DV II werden folgen.

Sicherheit am Arbeitsplatz

Die Sicherheit von auf einem privaten Endgerät verarbeiteten personenbezogenen Daten aus der Schule kann weiter verbessert werden, indem der Nutzer das Gerät selbst schützt. Es muss dafür gesorgt werden, dass Dritte gar nicht Zugriff auf das Gerät erhalten.

- Man lässt es in der Schule außerhalb des (in der Regel) sicheren Lehrerarbeitsplatzes im Lehrerzimmer oder Lehrerarbeitsraum nicht unbeaufsichtigt herumstehen bzw. -liegen. Über das Wochenende bzw. die Ferien sollte man private Endgeräte, auf denen personenbezogene Daten aus der Schule verarbeitet werden, entweder mit nach Hause nehmen oder in der Schule sicher wegschließen.
- Ausführliche Tipps für die Sicherheit des heimischen Arbeitsplatzes findet man auf der Seite des Bundesamtes für Sicherheit und Informationstechnik (BSI) zum IT Grundschutz - INF.8 Häuslicher Arbeitsplatz https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_8_H%C3%A4uslicher_Arbeitsplatz.html