Thomas Martin

Privat–Geräte im Dienstbereich,
Verzeichnis von Verarbeitungstätigkeiten,
Vertretungspläne im Internet

DATENSCHUTZ AN SCHULEN DES RHEIN-ERFT-KREISES

Thema: Privat-PC **im Dienst**

DA ADV- Anforderungen :

Die **professionellen** Anforderungen an die **Nutzung** der **privaten** Endgeräte im **Dienstbereich** …. gab es immer**.**

Sie haben ein Update im neuen **Runderlass 10 – 41 Nr.4**.

Siehe Formular **„DA ADV“** v. 19.01.2018, 11 Seiten

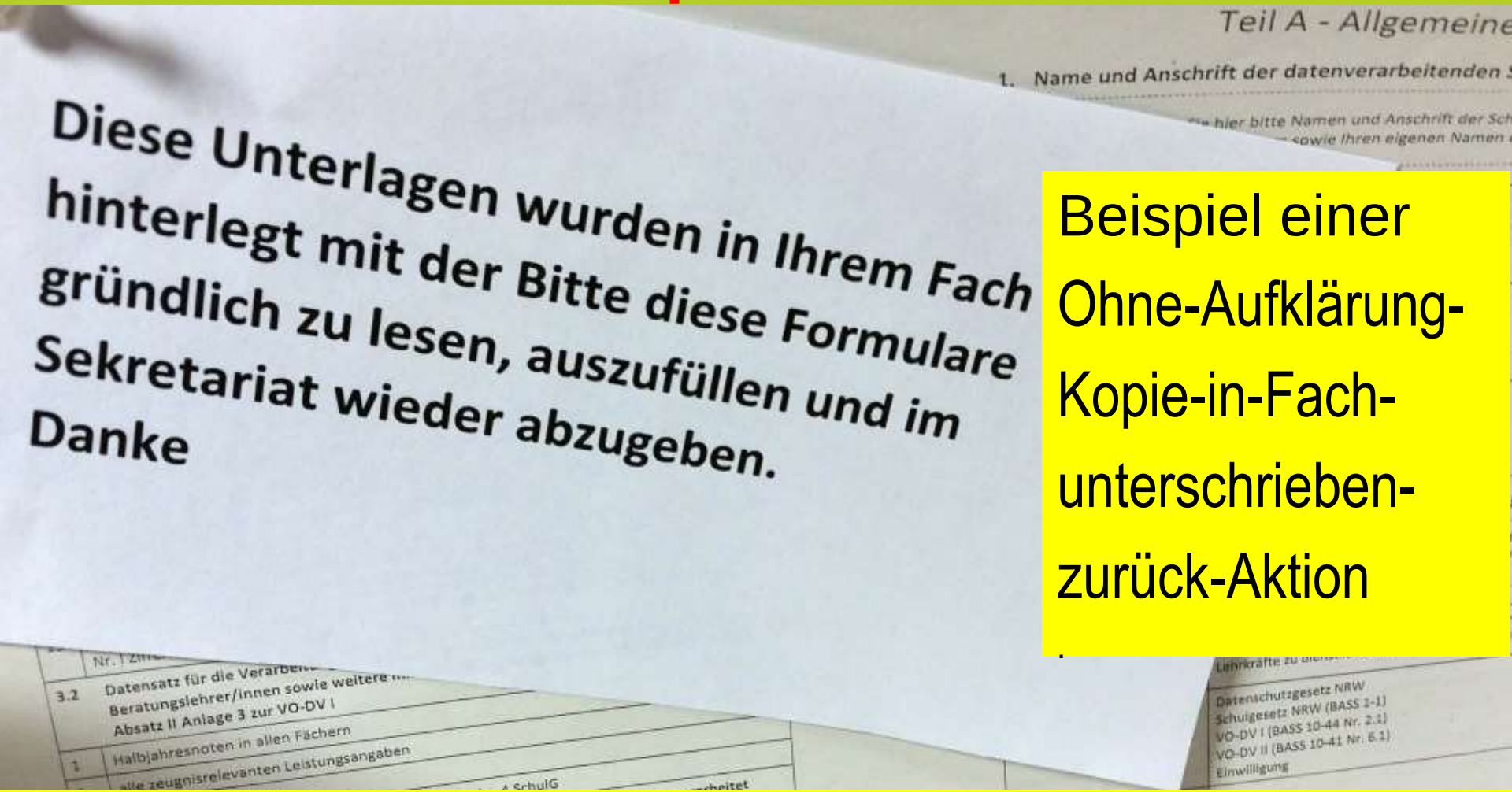
Teil A – Allgemeine Angaben	– Welche Daten darf wer verarbeiten
Teil B – Datensicherheit	– Hier geht es um praktische Schutzmaßnahmen
Teil C – Verpflichtungserklärung	– Arbeits- und haftungsrechtliche Konsequenzen

Sie + die SL sollen **a l l e s** verstehen, unterschreiben, umsetzen.

.

Thema: Privat-PC **im Dienst**

DA ADV- **Kopie-in-Fach: soo nicht!**



Beispiel einer Ohne-Aufklärung-Kopie-in-Fach-unterschrieben-zurück-Aktion

Aber es **gilt** weiterhin: Kein Lehrer*In MUSS sein Privatgerät im Dienstbereich einsetzen.

Thema: Privat-PC **im Dienst**

Teil **A+B** DA ADV- Anforderungen :

Administratoren für Dienstgeräte fehlt zu einem Genehmigungsverfahren z.B.:

→ an jedes Gerät angepasste **Prüfvorgaben und Prüfmöglichkeit** seitens SL und DSB.

Auch enthält das Formular **keine konkretisierten Angaben,** z.B. im **Teil B**:

Hinweise zu **Verschlüsselungsschutzanforderungen** nach aktuellem technischen Stand**:**

- Mindestens der Ordner mit den Schuldaten muss verschlüsselt sein → „Log-in“ alleine reicht nicht;
- benötigen wir zur Sicherheit weiterhin ein Bios-Passwort, ein Boot-Passwort oder auch einen Schutz der Userdaten einer Smartphone-App, damit sie Daten nicht weitergibt (z.B. an WhatsApp) etc.?
- zu unzulässiger Betriebs- und Software, z.B.: WhatsApp = no go, Office 365 Server speichert außerhalb.
- eine **Blacklist / Whitelist** der unzulässigen / zulässigen Software auf „dienstlichen“ Privat-Geräte.
- dass z.B. über Outlook **keine gemeinsame Verwaltung** von privaten + Dienst-eMails erfolgen darf.

Die **LDI** (Landesbeauftragte für Datenschutz und Informationsfreiheit) sagt im 23. Datenschutzbericht:

„Die **Schulleitung** ist aufgrund der Vielfältigkeit der Risiken bei der Datenverarbeitung heutzutage nicht mehr in der Lage, alle technisch relevanten Sicherheitsaspekte zu überschauen.“

Thema: Privat-PC **im Dienst**

Teil **B** - Datensicherheit nach § 10 DSG NRW:

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)
- **automatische Sperre** der privaten Endgeräte nach maximal 15 Minuten Inaktivität
- Anlegen eines **eigenen Benutzerkontos** für dienstliche Zwecke (sofern technisch möglich)
- Verschlüsselung der gespeicherten Daten durch ein geeignetes Verfahren z. B. bei externen Datenträgern
- Sofern LOGINEO NRW eingesetzt wird und erreichbar ist:
  Bearbeitung und Speicherung von Dokumenten, die sensible personenbezogene Daten (z.B. Wortzeugnisse) enthalten, ausschließlich über den **Online-Editor von LOGINEO NRW**.

DSG NRW, **§** 10 Technische und organisatorische Maßnahmen**:** Auszug **Abs.3:**

Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklungen der Technik zu überprüfen.

Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen.

Thema: Privat-PC **im Dienst**

Teil **B** - Datensicherheit nach § 10 DSG NRW:

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
- Einsatz **aktueller Virenschutz-Software**
- Einsatz einer **Firewall**

3. Verfügbarkeit

Damit die Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können, ergreife ich folgende Maßnahmen:

- **regelmäßige Aktualisierung** der (Betriebs-)Systeme
- **regelmäßige Aktualisierung** eingesetzter Anwendungen (z.B. Virendefinitionen)
- **regelmäßige Backups** der verarbeiteten Daten

DSG NRW, **§** 10 Technische und organisatorische Maßnahmen**:** Auszug **Abs.3:**

Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklungen der Technik zu überprüfen.

Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen.

Thema: Privat-PC **im Dienst**
Teil **C** DA ADV- Anforderungen :

Teil C – Verpflichtungserklärung

Ihre Unterschrift unter der Verpflichtungserklärung ist notwendig, damit Sie Ihre privaten Geräte für dienstliche Zwecke nutzen können. Sie bestätigen damit, dass Sie alle Inhalte dieser Erklärung verstanden haben und die aufgeführten Maßnahmen umsetzen werden.

Ich verpflichte mich, ausschließlich die in Teil A (und ggf. E) genannten personenbezogenen Daten auf meinen privaten Endgeräten und die Daten auch nur für dienstliche Zwecke zu verarbeiten. Des Weiteren verpflichte ich mich, die in Teil B aufgeführten technischen und organisatorischen Maßnahmen umzusetzen und einzuhalten.

Ich werde jegliche Änderung der obenstehenden Angaben der/den datenverarbeitenden Stelle/n zur Kenntnis bringen. Ich wurde darüber in Kenntnis gesetzt, dass ich verpflichtet bin, der Schulleiterin oder dem Schulleiter alle Auskünfte zu erteilen, die für die datenschutzrechtliche Verantwortung erforderlich sind.

Ich verpflichte mich, Datenmissbrauch oder Datenverlust der bei mir verarbeiteten Daten umgehend der Schulleitung zu melden.

Ort, Datum Unterschrift der Lehrkraft

Die **SL** muss VORHER aufklären, z.B. über mögliche Haftungsfolgen (arbeits-/disziplinarrechtliche etc.).
Die SL ist persönlich verantwortlich für Personendaten der Schule, wo immer sie verarbeitet werden!
Sie sollte z.B. dokumentieren, wann LuL nach relevanten Veränderungen am Privatgerät befragt wurde.

Thema: Privat-PC **im Dienst**
Teil **D** DA ADV- Anforderungen :

Teil D – Genehmigung der Schulleiterin / des Schulleiters

Die Unterschrift der Schulleiterin/des Schulleiters unter der Verpflichtungserklärung ist notwendig, damit Sie Ihre privaten Geräte ab dem unter Teil A genannten Zeitpunkt für dienstliche Zwecke nutzen dürfen. Darüber hinaus besteht nur auf diese Weise ein Haftungsschutz für die in Teil B aufgeführten Geräte.

Unter den oben genannten Voraussetzungen erteile ich die Genehmigung zur Verarbeitung der in Teil A genannten Daten zu dienstlichen Zwecken auf den unter Teil B, Absatz 2.5 genannten privaten Endgeräten der Lehrkraft.

Ort, Datum **Unterschrift**

Die SL muss VORHER aufklären, z.B. über den Haftungsschutz des privaten Gerätes oder mögliche Haftungsfolgen bei Verstößen oder falscher Handhabung (arbeits-/disziplinarrechtliche etc. Folgen).
Die **SL** kann die Dienststelle um Hilfestellung / Aufklärung **vor** Genehmigung ersuchen.

Das **OLG Hamm stellte am 9.3.2018** fest, dass die SL alle Verarbeitungsarten von Personendaten tatsächlich prüfen und dokumentieren muss. Die SL ist für die Personendaten ihrer Schule verantwortlich und evtl. bei grober Fahrlässigkeit / Vorsatz persönlich haftbar.

Genehmigungsformular + **ToDo für SL**

Voraussetzung für den Privat-PC-Einsatz sollte sein:

Angaben + Fragen zum Einsatz vorab abprüfen und dokumentieren, z.B.**:**

- Schule **führt** das alte **Verfahrensverzeichnis** weiter bzw. erstellt nach DSGVO Art. 30 ein neues **Verzeichnis der verarbeitenden Verfahren** (und hat das mit dem DSB beraten).
- **Trennung** von **Verwaltungsnetz** und **pädagogischem Netz –** nur ein sicheres Netz gefährdet keine anderen Geräte z.Bsp. die eingebundenen Privat-Geräte.
- **Verhaltensbezogene** Software mit Personalvertretungen abgeglichen (z.B. nach § 72 LPVG etc.)
- Abfrage der **Erforderlichkeit** (laut LDI): besonderen **Grund anführen** für den Privat-Geräte-Einsatz:
- Hat die Schule fehlende **Verwaltungsrechner beim Schulträger** und fehlende **Dienstrechner beim zuständigen Schulamt bestellt**?
- Eine Blacklist und eine Whitelist für die nicht zulässige bzw. zulässige Soft- und Hardware wurde beim Dienstherrn angefordert.
- **Haftungsbereiche** sind geklärt: z.B. bei Schädigung eines Privat-Gerätes durch eine Virenversendung aus dem Verwaltungsnetzwerk, kommt die Schule für die Reparaturkosten auf.

FRAGE: Kann eine Schulleitung kategorisch unsichere Privat-Geräte für den Diensteinsatz genehmigen, wenn sie das **eigene Verwaltungsnetzwerk nicht gesichert und legitimiert** hat?
IT-Sicherheit und Datenschutzsicherheit müssen geprüft und dokumentiert sein (z.B. DSGVO Art. 30+35).

Fragen um den Privat-PC-Einsatz:

Einige typische Problemsituationen mit Privat-Geräten in Schule

- \+ Kein Einsatz von Privat-Geräten – alle pbD-PC-Arbeiten geschehen auf Schulverwaltungsrechnern
- \+ Einsatz von Privat-Geräten UND keine personenbezogene Datenverarbeitung (=pbD)
- \+ Genehmigter Einsatz von Privat-Geräten UND personenbezogene Datenverarbeitung
- \- Ungenehmigter Einsatz von Privat-Geräten UND personenbezogene Datenverarbeitung
- ? Ungenehmigter Einsatz von Privat-Geräten UND personenbezogene Datenverarbeitung UND die SL sendet dennoch die eMail-Einladungen zur Konferenz an die Lehrperson
- \+ Genehmigtes Privat-Gerät UND Einsatz von im Unterricht
- \- Ungenehmigter Privat-Gerät UND Einsatz von im Unterricht
- ? Genehmigtes / ungenehmigtes Privat-Gerät im Unterricht UND es passiert ein GAU: falsche Personendaten, Prüfungsaufgaben oder eine unziemliche Internetseite poppen im Beamer auf.
- ? Verschlüsselte USB-Sticks legitimieren weder das Schreiben von Gutachten, AOSF, Förderpläne o.ä. auf genehmigten Privat-Geräten, noch „genehmigt“ ihr Einsatz ungenehmigte Privat-Geräte.
- \+ Ein Elternteil fragt die SL, was das Bild des Kindes im Privat-Gerät des L. tut (Art. 15 DSGVO)

BEACHTE: Sowohl die Schulleitung als auch die LuL untergraben ihre Rechtsposition, falls sie falsche bzw. ungenehmigte Zustände wissentlich dulden.

Beispiel Schul-Verwaltungsnetz + Privat-Geräte

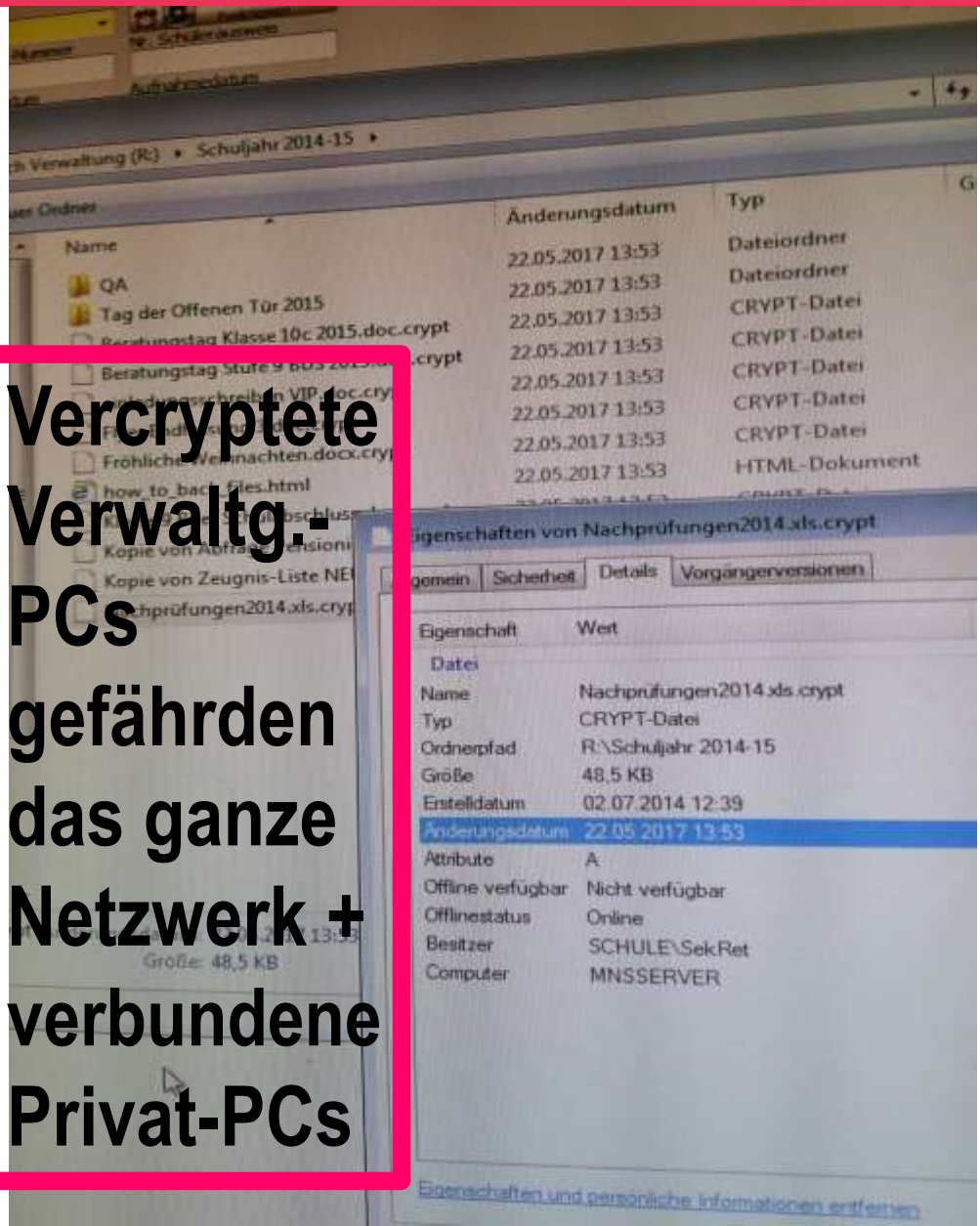
Anforderungen an das **Verwaltungsnetz:**

Das **Verwaltungsnetzwerk** muss definiert abgesichert sein und nur dienstuntergebene, zugewiesene und ausgebildete Personen dürfen zugreifen.

Der Vertrag mit den Dienstleistern (z.B. fürs Schulnetzwerk) müssen auch die SL in Weisungsfunktion setzen. Die **Schulleitung** ist **haftend** eingebunden wenn es um Personendaten der Schule geht, wo immer sie verarbeitet werden (eigene Kontrollmaßnahmen dokumentieren).

Die Folge ungeprüfter Netzwerke:

Eine SL kann keine Privat-Geräte genehmigen, wenn sie kein „altes“ Verfahrensverzeichnis bzw. neues Verzeichnis von Verarbeitungstätigkeiten (s. Art. 30 + 35 DSGVO) o.ä. führt.



Vercryptete Verwaltg.-PCs gefährden das ganze Netzwerk + verbundene Privat-PCs

Thema: Privat-PC **im Dienst**

Kommentar: DA ADV- Anforderungen:

Da es keine Dienstgeräte und genügend Verwaltungsrechner gibt, hat Schule ihre Arbeitsfähigkeit trotz des rasanten technischen Wandels erhalten, indem sie (die Schulverwaltung/Schulträger) sich an den Einsatz von **nicht zertifizierten Privatgeräten** im Dienst als Standard **„gewöhnt“** hat.

In diesem Zusammenhang würde es Sinn machen, wenn …

- Dezernenten / SR jährlich den Status des Datenschutzes / der IT-Sicherheit abfragen würden,
- die QA feststellen würde, wieweit Datenschutzmaßnahmen und IT-Sicherheit den schützenden Rahmen aller täglich Personendaten-Arbeiten von LuL und SL bilden

Wer steuert diese Gerätediversität, diese „TÜV-Losigkeit“ ?

Ein heute kaum noch regelbarer digitaler Wildwuchs überfordert Lehrkräfte, Schulleitung, Schulverwaltungen und Schulträger.

Das **Dilemma** ergibt sich aus dem **versuchten Einhalten**…

- des unstrittig notwendigen Datenschutzes in Schule,
- der weiter steigenden professionellen Anforderungen („Digitalisierung“)

→ bei gleichzeitigem **Verweigern** von ausreichend Verwaltungsrechnern und Dienstgeräten als Standard für LehrerInnen durch den **Dienstherrn / Schulträger**, der weiter auf der Basis subventionierter + unsicherer **Privatgeräte** den Schulbetrieb plant.

Thema: Vertretungspläne …außerhalb des Lehrerzimmers

Dürfen Vertretungspläne im Schulgebäude und/oder auf der Schulhomepage, im Intranet zugänglich sein?

Die ordnungsgemäße Aufgabenerfüllung der Schule bedingt die am Schulleben beteiligten Schüler, Eltern und Lehrkräfte über Stundenplanänderungen mittels eines Vertretungsplans zu informieren.

Problem:

Auch ohne Nennung der zu vertretenden bzw. die Vertretung übernehmenden Lehrkraft (Namen oder Namenskürzel) kann eine Personenbeziehbarkeit des Vertretungsplans (welche Lehrkraft wird vertreten) nicht ausgeschlossen werden.

Thema: Vertretungspläne …außerhalb des Lehrerzimmers

Vertretungsplan für...	Was ist sichtbar?	Wo: Intranet	Wo: Internet
Schülerinnen und Schüler **[gute Lösung]**	• nur die Vertretungen der eigenen Klasse • keine personenbezogenen Daten wie Namen oder Kürzel z.B. **5a – Deutsch – 3. Std. – Vertretung**	Jede Klasse hat ihren eigenen Benutzernamen und ihr eigenes Klassenpasswort.	Eine weltweite Veröffentlichung im Internet (z.B. Homepage) verbietet sich in Ermangelung der Erforderlichkeit. ➔ Der Vertretungsplan muss nicht über den Kreis der am Schulleben Beteiligten öffentlich gemacht werden. Die Aufgabe des Unterrichtens ist erfüllt – es gibt keine weitere „Erforderlichkeit“. **➔ = keine juristische Handhabe zur „App“.**
Schülerinnen und Schüler **[kritisch]**	• nur die Vertretungen der eigenen Klasse • mit personenbezogenen Daten (Namenskürzel) z.B. **5a – Deutsch – 3. Std – Vertretung: Mü - Raum 212**	Jeder Schüler hat seinen eigenen Benutzernamen und sein eigenes Passwort.	
Lehrkräfte	• Alle Vertretungen sind aus dienstlichen Gründen für alle Lehrkräfte sichtbar. • mit personenbezogenen Daten (Namenskürzel)	Jede Lehrkraft hat ihren eigenen Benutzernamen und ihr eigenes Passwort.	

Fragen gerne jetzt oder später

Danke für Ihr Interesse!

Thomas Martin

Datenschutzbeauftragter
an Schulen
des Rhein-Erft-Kreises

TOM211007@web.de

QR-Code scannen