oead DIGITALES LERNEN

Digitale Schule – Digitales Lernen

Organisatorisch-rechtliche Rahmenbedingungen der Geräteinitiative

Wien, 14. Oktober 2021

Pädagogische Hochschule Steiermark

Bundesministerium Bildung, Wissenschaft und Forschung

Während des Webinars

- Stellen Sie bitte Ihre Mikrofone ab!
- Fragen Sie gerne jederzeit schriftlich
- Die Veranstaltung wird **NICHT** aufgezeichnet
- Melden Sie sich zu unserem Newsletter an!

Ablauf

- Anrechnung des Webinars an der PH Steiermark
- Einleitung und Erklärung Geräteinitiative
- Kurzer Überblick zu den gesetzlichen Grundlagen der Geräteinitiative:
  - **Bundesgesetz zur Finanzierung der Digitalisierung des Schulunterrichts (SchDigiG)**
  - **Schulunterrichtsgesetz (SchUG)** insb. §14a und 18b
- Datenschutz: Rechtsgrundlagen
- Datenschutz: Cloud & MDM
- IKT-Schul-VO
- Digitale Endgeräte & häuslicher Unterricht
- Fragen und Antworten
- Abschluss

Anrechnung des Webinars als Fortbildung an der PH Stmk.

- Stellen Sie sicher, dass Sie an der PH Steiermark immatrikuliert sind
- Anleitung Immatrikulation an weiteren PHn unter: https://bit.ly/3dRGgM6
- Anmeldungen sind **bis 14.10.2021** möglich
- Teilnahmebestätigungen werden am 15.10.2021 versendet

Portal Digitale Schule

Einheitliche Kommunikationsprozesse

Distance-Learning-MOOC

EDUTHEK
Ausrichtung der Eduthek nach Lehrplänen

Gütesiegel LernApps

Ausbau der schulischen Basis-IT-Infrastruktur

Digitale Endgeräte für Schülerinnen und Schüler

Digitale Endgeräte für Lehrerinnen und Lehrer

www.digitaleschule.gv.at

Der OeAD als Ihr Ansprechpartner der Geräteinitiative

- Informationen zur Geräteinitiative auf unserer Homepage digitaleslernen.oead.at
- FAQs des OeAD
- Schreiben Sie dem OeAD: digitaleslernen@oead.at
- Zum OeAD Digitales Lernen Newsletter anmelden

oead DIGITALES LERNEN

Präsentation der rechtlich-organisatorischen Aspekte des 8-Punkte-Plans

MinR Dr. Thomas Menzel

Pädagogische Hochschule Steiermark

Bundesministerium Bildung, Wissenschaft und Forschung

Bundesministerium
Bildung, Wissenschaft
und Forschung

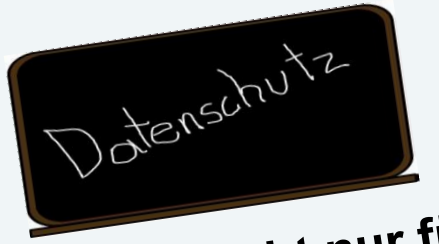
Datenschutz
Informationssicherheit

datenschutz@bmbwf.gv.at

MinR Dr. Thomas Menzel, R Ing. Andreas Laschalt, BSc
BMBWF, Datenschutzbeauftragter, Bereich Bildung
Oktober, 2021

Datenschutz Grundsätze

Warum Datenschutz in der Schule ?



- Die Verwendung der Daten von Schüler/innen wird aufgrund neuer Technologien für den Unterricht immer wichtiger
- Unternehmen beuten Daten von Schüler/innen zunehmend aus
- Die Schüler/innen haben ein Recht darauf, dass auch die Lehrer/innen ihre Daten schützen

Datenschutz ist nicht nur für die Schulverwaltung und IT-Administratoren sondern für jede Lehrerin und jeden Lehrer wichtig!

Bsp für datenschutzkonformes Verhalten

- Passwörter nicht weitergeben
- Klassenbucheintragungen nicht vorlesen
- Klassenlisten mit Synonymen wenn sinnvoll (Echtnamen nicht in Gratisanwendungen wie Dropbox)

Was kann ich als Lehrkraft tun?

- ✓ **Bewusstsein**: Wann und in welchem Zusammenhang verwende ich Daten von Schüler/innen?
- ✓ **Weitergabe**: Wem gebe ich die Daten weiter und wieso?
- ✓ **Sicherheit**: Wie verhindere ich, dass die Daten in falsche Hände geraten?
- ✓ **Apps**: Mit welchen Apps arbeite ich? Sammeln Firmen dabei Schülerdaten?
- ✓ **Löschen**: Daten sollen nicht gesammelt werden!. Lösche ich die Daten, wenn ich sie nicht mehr brauche?

datenschutz@bmbwf.gv.at

Schullandschaft in Österreich

- Zentralstelle BMBWF
- 9 Bildungsdirektionen, Bifie
- Ca. 550 Bundesschulen – 56.000 bundesbedienstete Lehrer/innen
- Ca. 6000 Schulen – 120.000 Lehrer/innen
- Ca. 1,1 Mio Schüler/innen

Grundsätze der Datenverarbeitung Art. 5 DSGVO

1. TRANSPARENZ

Information welche Daten verwendet werden

Bsp: Information der Schüler/innen bzw Eltern über eLearning Tools und die damit verbundene Verwendung von Daten

2. ZWECKBINDUNG

ZWECK

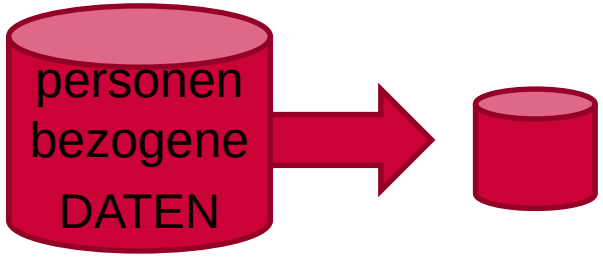
Nur Daten für einen Zweck verwenden!

Keine Weitergabe!

Bsp: Werbung ist ein anderer Zweck als Unterrichtsverwaltung!

Daten von Schüler/innen sind nicht für Werbezwecke weiterzugeben.

3. DATEN-MINIMIERUNG



Nur jene Daten speichern die notwendig sind!

Bsp: Lernplattformen wählen, die auf Datenschutz achten. Daten auf Lernplattformen löschen, wenn nicht mehr notwendig.

4. Treu & Glauben, rechtmäßig

5. Zeitliche Speicherbegrenzung

datenschutz@bmbwf.gv.at

Rechtsgrundlage der Datenverarbeitung Art. 6 DSGVO

1 Ausdrückliche gesetzliche Grundlage (BilDokG, SchUG)

Beispiele:
- ✓ Schülerstammdaten
- ✓ Klassenbuch
- ✓ Prüfungsprotokolle

2 zur Wahrnehmung einer gesetzlich übertragenen Aufgabe im öffentlichen Interesse

Beispiele:
- ✓ Lernplattform
- ✓ Organisation einer Projekt-woche

3 Lebenswichtiges Interesse (medizinischer Notfall)

Schüler/in

personenbezogene DATEN

Lehrer/in

ACHTUNG:

OHNE GESETZLICHE GRUNDLAGE IST

DIE EINWILLIGUNG ZUR DATENVERWENDUNG NOTWENDIG

datenschutz@bmbwf.gv.at

Datenschutz-Schnellprüfungsschema (DS-SPS)

1) Werden personenbezogene Daten verarbeitet?

Personenbezogene Daten, Verarbeitung

2) Darf ich diese Daten verarbeiten?

↳ Rechtsgrundlage, Grundsätze

3) Was muss ich dabei beachten?

↳ TOMs, DVV, AVV ...

Datenschutz Basic Check

I. Darf ich personenbezogene Daten verarbeiten?

- Es bedarf einer Grundlage iSd Art 6 DSGVO (bzw bei Daten besonderer Kategorien iSd Art 9 DSGVO), in der hoheitlichen Verwaltung kommt dabei insbesondere eine gesetzliche Grundlage in Betracht.
- Es sind nur jene Daten und nur so zu verarbeiten, wie es die datenschutzrechtlichen Grundsätze (siehe insbes. Art 5 DSGVO) zulassen. An dieser Stelle seien insbesondere die Prinzipien der Datenminimierung und Zweckbindung hervorgehoben.

Datenschutz Basic Check

II. Wenn ich personenbezogene Daten verarbeite, was muss ich dabei u.a. beachten?

- Datensicherheitsmaßnahmen nach Art 32 DSGVO
- Informationspflichten nach Art 13 und 14 DSGVO
- Eintrag ins bzw. Aktualisierung des Datenverarbeitungsverzeichnis nach Art 30 DSGVO
- Umstände schaffen, die die Wahrung der Betroffenenrechte nach Art 12 DSGVO ermöglichen
- ggf. Auftragsverarbeitervereinbarung nach Art 28 DSGVO
- ggf. Vereinbarungen bei gemeinsamen Verantwortlichkeiten nach Art 26 DSGVO

Einwilligung - Formular

Nur nötig, soweit keine Verarbeitung aufgrund gesetzlicher Grundlage erfolgt
(zB: Mail-Adresse Schüler/in, Marketing/Schulhomepage, Kopierkarten, Essensausgabe etc)

„Ich, xxx (Name, Adresse) stimme zu, xxx

dass meine persönlichen Daten, - ODER , dass die personenbezogenen Daten meines xxx, Name xxx,

nämlich [Datenarten aufzählen, zB Name, Adresse, Geburtsdatum …]

zum Zweck der

[genauen Zweck anführen,]

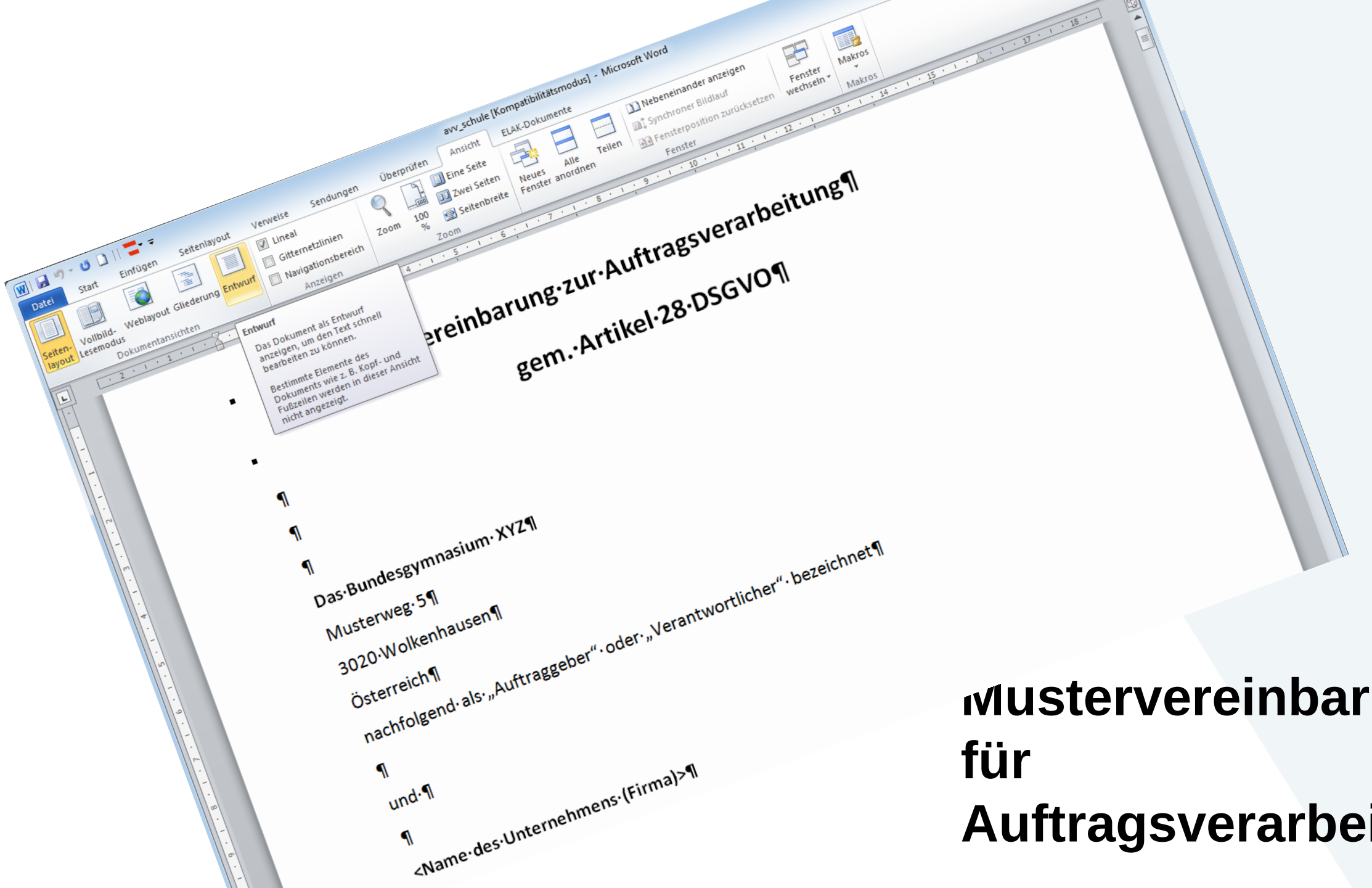
verarbeitet werden und

an

[Anführung des/der genauen Übermittlungsempfänger(s), zB XY GmbH]

zum Zweck der [genauer Übermittlungszweck] übermittelt werden.

Diese Einwilligung kann ich jederzeit schriftlich mittels Brief an die Schulleitung (Name der Schule, Adresse) widerrufen.



Mustervereinbarung für Auftragsverarbeiter

DATENSCHUTZ – DATENSICHERHEIT

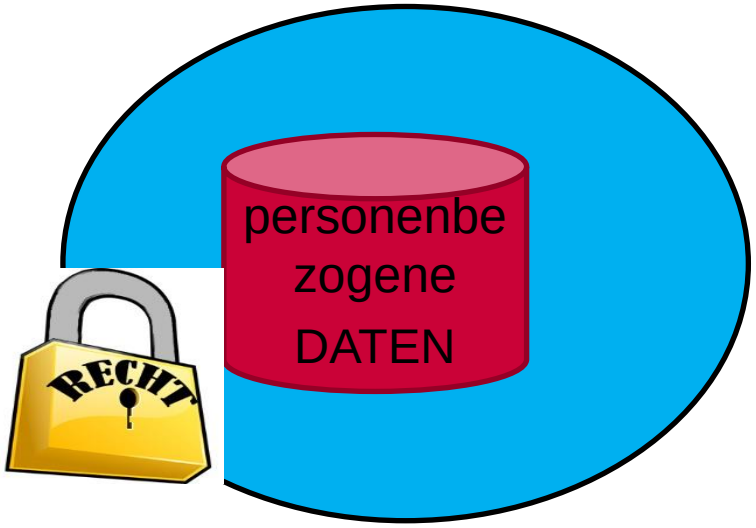
Datenschutz =

Rechtlicher Schutz

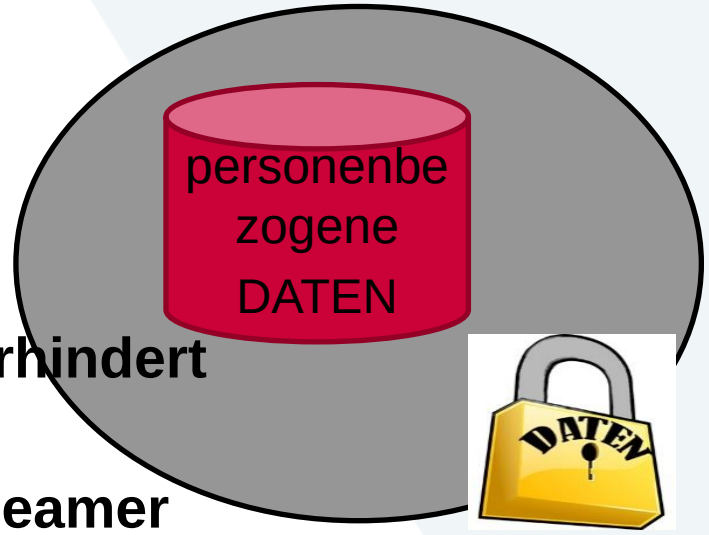
Datensicherheit =

Technischer Schutz, organisatorische / menschliche Maßnahmen

KEIN DATENSCHUTZ OHNE DATENSICHERHEIT!



- **Passwörter nicht weitergeben**
- **ausloggen nicht vergessen**
- **Verschlüsselter USB-Stick**
- **USB-Stick auf Schlüsselbund (verhindert Liegenlassen)**
- **Keine Klassenbucheinträge auf Beamer sichtbar machen**
- **Brochure „Sind Sie sicher ?“ des BMBWF**



Kategorien von Verarbeitungstätigkeiten an Bundesschulen

- **Verwendung sozialer Netze (zB Whatsapp Facebook)**

  - für schulbezogene Eltern-Lehrer-Schüler-Kommunikation sowohl aus datenschutzrechtlichen als auch aus lizenzrechtlichen Gründen generell nicht zulässig
  - geeignete spezielle Angebote können durch die Schule beauftragt werden
    edu.flow, schoolfox, schoolupdate, Web-Untis-Schüler/Elternzugang
    Matrix/Riot-Server lokal an der Schule
  - Reiner Privatgebrauch fällt nicht in Regelungskompetenz der Schule (außer etwa Hausordnung, SaferInternet beachten)

Kategorien von Verarbeitungstätigkeiten an Bundesschulen

- **Dienstliche E-Mail-Postfächer für Lehrer/innen**
  - Vorname.nachname@bildung.gv.at verpflichtend für Bundeslehrer/innen
    - Rechtsgrundlage § 5 BD-EG, Dienstrecht
    - Auftragsverarbeiter in der BRZ (Hosting in eigenem Tenant in Office365)
    - Auftragsverarbeitervereinbarung diesbezüglich 2017 abgeschlossen
  - Schulbezogene Postfächer für Lehrer/innen
    - Vorname.nachname@BG-entenhausen.at , thema@BG-entenhausen.at
    - Zulässig, entscheidung am Schulstandort
    - Rechtsgrundlage § 5 BD-EG, Dienstrecht
    - Private Clouddienstleister zulässig, soweit Auftragsverarbeitervereinbarung vorliegt mit dem Schulstandort vorliegt
    - Generelle Vereinbarung zwischen BMBWF und Apple, Google, Microsoft liegt vor

Beispiel: HowTo DSGVO (HTL Spengergasse)

How to … DSGVO @ HTL Spengergasse (aktualisierte Version)

„Ich will, dass mit meinen Daten sensibel umgegangen wird!“

Die DSGVO gilt für die digitale oder manuelle Verarbeitung (kopieren, löschen, speichern, verändern, ...) von personenbezogenen Daten (z.B. Vorname, Nachname, Geburtsdatum).

Datenanwendungen (z.B. Anmeldeverfahren, WebUntis):
für die Administration und Verwaltung des Schulalltags werden von der Schule an das BMBWF gemeldet.

Wie soll ich die DSGVO persönlich umsetzen?		**Technische und organisatorische Maßnahmen werden von der Schule getroffen, um die Daten zu schützen**
Manuelle Verarbeitung	Digitale Verarbeitung	
z.B. Schularbeiten, Tests, Lehrendenhandbücher, Schülerlisten	z.B. Laptop, SchulPC	
* Aufbewahrung der Daten in der Schule (Lehrendenzimmer)	* Speicherung der Daten auf den Schullaufwerken * Nutzung des VPN-Services des ZID zum Schullaufwerk	

wenn ich die Daten **privat** digital und manuell verarbeite ...	**... muss ICH alle technischen und organisatorischen Maßnahmen treffen, damit die Daten geschützt werden**

NO GO:	**LÖSUNG:**
Personenbezogene Daten (auch Foto) über soziale Medien (Facebook, WhatsApp, usw...) verteilen oder in Cloud-Services (Dropbox, OneDrive, usw...) speichern.	Nutzung der ZID-Services (z.B. E-Mail oder cloud.spengergasse.at) zur Speicherung oder Verteilung. Bitte Zustimmung bei Fotos einholen!

Vorlesen von Noten im Klassenraum:
Derzeitige Rechtsmeinung BMBWF: Bei mündlichen Prüfungen ja, bei schriftlichen Prüfungen nein (auch keine gesammelte Bekanntgabe der Noten via E-Mail-Klassenverteiler)

Datengeheimnis (gilt auch nach Beendigung des Dienstverhältnisses):
Keine personenbezogenen Daten digital (Klassenverteiler) oder manuell (Aushang in der Klasse) an andere Personen schicken, weil …

... „auch ich will, dass man mit meinen Daten sensibel umgeht!“

datenschutz@bmbwf.gv.at

Rene Pranz, Nenad Subotic
HTL Spengergasse, März 2019

Weitere Aspekte

- Automatisierte Löschung bzw Take-Out-Tools nach Schulende
- Experten zu den Cloud-Produkten in den Pädagogischen Hochschulen
- Technologiebeobachtung durch diese Experten
- Device Management für Geräte und Cloud-Accounts an den teilnehmenden Schulen
- Datenschutzfreundliche Voreinstellungen auf Schüler-Tablets (Cookie, Ad-Tracking, Geo-Daten, Encryption etc)
- Datenschutzschulung mit Schwerpunkt für Schulleiter/innen und Lehrer/innen
- Awarenessbildung zu Datenschutz & Cloud im Unterricht
- Verankerung des Datenschutzes in Lehrplänen, Lehrerausbildungs-Curricula und in der Schulleiterausbildung

datenschutz@bmbwf.gv.at

Rechtliche Themen

Übersicht: Rechtliche Themen

- Datenschutz: Rechtsgrundlagen
- Datenschutz: Cloud & MDM
- IKT-Schul-VO
- Digitale Endgeräte & häuslicher Unterricht

Datenschutz: Überblick Rechtsgrundlagen

- Rechtlich gesehen sind bezüglich des Datenschutzes in Schulen hohe Standards gewährleistet:
  - Es wurde eine neue gesetzliche Grundlage zum IKT-gestützten Unterricht in § 14a SchUG geschaffen und ein verstärktes Augenmerk auf Datenschutz in § 4 BilDokG 2020 sowie auf IT-Sicherheit in § 6 Z. 1 SchDigiG gelegt.
  - In Anlage 2 des Bildungsdokumentationsgesetzes 2021 (BilDokG) wurde eine gesetzliche Grundlage für die erforderlichen Datenverarbeitung zur Durchführung von Distance Learning und der Verwaltung von Schülerendgeräten geschaffen.
  - Eine Verordnung zur Datensicherheit in der Schul-IT (IKT-SchulVO), die mittels technischer und organisatorischer Maßnahmen die oben genannten gesetzlichen Regelungen konkretisiert, wurde im August 2021 kundgemacht (BGBl. II Nr. 382/2021).
  - Ältere Normen: Schülerausweis (§ 57b SchUG), Klassenbuch (§ 77 Abs. 3 SchUG), Dienst-Mail (§ 5 Abs. 6 BD-EG), teilweise Direktwirkung des E-Government-Gesetzes
  - Nähere Informationen zur gesetzlichen Gewährleistung von Datenschutz in Schulen sind auf der Website des Bildungsministeriums einsehbar: Datenschutz in Schulen

Datenschutz: Grundsätze zu Cloud & MDM

- Im Zuge der Schulverwaltung an österreichischen Schulen erfolgt grundsätzlich keine Datenübermittlung an Staaten außerhalb der EU. Insbesondere US-basierte Clouddiensteanbieter werden nicht im Rahmen der Schulverwaltung eingesetzt.
- **Cloud-Dienste** mit denen durch das BMBWF eine datenschutzrechtliche Vereinbarung abgeschlossen wurde, werden nur dann verwendet, wenn spezielle Datenschutzgarantien für den Bildungsbereich abgegeben wurden (zB keine zielgerichtete Werbung durch die Cloudiensteanbieter und generell Verarbeitung der Daten nur nach Weisung der verantwortlichen Schule; Clouddiensteanbieter ist Auftragsverarbeiter, keine Schulverwaltung).
- **Mobile Device Management** (MDM gem. § 6 Z. 1 SchDigiG) ist zum Schutz der Schüler/innen-Daten am Schulstandort und der IT-Sicherheit im Schulnetz erforderlich und gewährleistet aktuelle Softwarekomponenten, wie etwa Virenschutz am Endgerät.
- **Fernverwaltung** gem. § 6 Z. 2 SchDigiG: Lehrer/innen dürfen nur in der konkreten Unterrichtssituation auf Schüler/innen-Geräte zur Unterstützung der teilnehmenden Schüler/innen bzw. zur Gewährleistung der pädagogischen Unterrichtsziele zugreifen. Dieser Zugriff ist den jeweiligen Schüler/innen deutlich anzuzeigen. ()

IKT-Schul-VO

- VO am 31. 8. im BGBl veröffentlicht (BGBl. II Nr. 382/2021)
- Grundsatz: keine neuen Anforderungen, sondern nur Zusammenfassung bestehender Normen

- Wesentliche Regelungsinhalte:
  - Kategorien Verarbeitungstätigkeiten (Schulverwaltung, Pädagogik, schulbezogene IT-Services)
  - Authentifizierung (Schulverwaltung: 2Faktor)
  - Bildungsstammportale
  - Hosting (inkl. Rahmenbedingungen Cloud)
  - Endgeräteverwaltung
  - Organisatorischer Datenschutz
  - IT-Nutzungsbedingungen
  - Video und Co im IT-gestützten Unterricht
  - Datenschutzrechtliche Verantwortlichkeit

Update zur IKT-Schul-VO: § 4: Begriffe

- **Schulverwaltung**: sämtliche Verarbeitungen personenbezogener Daten, die in datenschutzrechtlicher Verantwortung der Schulleitung am Schulstandort aufgrund schulgesetzlicher Regelungen vorzunehmen sind, soweit sie nicht in den Z 3 bis 6 geregelt sind; insbesondere
  - Evidenzen gemäß § 5 BilDokG 2020 dazu gehören jedenfalls alle IT-Systeme und Dienste, soweit deren Benutzerinnen und Benutzer, insbesondere in der Rolle der Schulleitung oder Sokrates-Administration damit schulweit auf personenbezogene Daten von Schülerinnen und Schülern zugreifen können, oder die überwiegend zur Verwaltung personenbezogener Daten nach Art. 9 Abs. 1 DSGVO eingesetzt werden,
  - Datenverbund der Schulen gemäß § 6 BilDokG 2020,
  - Ausstellung von Zeugnissen,
  - Stundenplanerstellung, Personalverwaltung, aktenmäßige Kommunikation zwischen Schule und Schulbehörde;
- unter dem Begriff „**Endgeräteverwaltung** (**Mobile Device Management**)“: ein IT-System zur zentralisierten Verwaltung von digitalen Endgeräten gemäß Z 10; dieses IT-System dient der Erfüllung der in § 10 festgelegten Funktionalität;
- unter dem Begriff „**Unterrichtsdokumentation**“: sämtliche Verarbeitungen von Schülerinnen- und Schülerdaten, die zu Zwecken der laufenden Dokumentation des Unterrichts und der Leistungsbeurteilung durch die Lehrperson vorgenommen werden sowie Datenverarbeitungen zur Durchführung von Kompetenzerhebungen;
- unter dem Begriff „**Fernverwaltung**“ (Classroommanagement): der Zugriff von Lehrpersonen auf die Schülerinnen- und Schülergeräte während des IKT-gestützten Unterrichts

§ 9: Organisatorische Datensicherheitsmaßnahmen

Die Schulleitung hat sicherzustellen, dass

1. Datenverarbeitungen gemäß § 4 Z 1 vor unbefugter Einsicht geschützt sind,
2. der Zutritt zu Räumen, in denen solche Datenverarbeitungen stattfinden, nur befugten Benutzerinnen und Benutzern möglich ist und bei etwaigem Parteienverkehr in diesen Räumen keine Einsichtnahme in die Daten erfolgen kann,
3. Datenverarbeitungen gemäß § 4 Z 1 bis 4 nur durch Bedienstete der eigenen Dienststelle nach Abwägung der Erforderlichkeit für die Erfüllung der schulrechtlich vorgesehenen Zwecke möglich sind, und nur diesen die dafür erforderlichen Zugangsberechtigungen eingeräumt werden,
4. Bedienstete der eigenen Dienststelle in regelmäßigen Abständen über die Bestimmungen der DSGVO und des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999, belehrt werden, insbesondere hinsichtlich
    a. der Wahrung des Datengeheimnisses gemäß § 6 DSG,
    b. der datenschutzrechtlichen Zweckbindung, auf deren Grundlage personenbezogene Daten nur für die schulrechtlich vorgesehenen Zwecke verarbeitet werden, dürfen sowie
    c. des Inhalts dieser Verordnung.

§ 12: IKT Nutzungsbedingungen

Unter Berücksichtigung der Anforderungen des § 11 ist die Verwendung eines digitalen Endgerätes im Schulnetz als Arbeitsmittel im IKT-gestützten Unterricht, zum eigenständigen Lernen und für Zwecke der Schulverwaltung zulässig.
Unzulässig ist:

1. eine Verwendung für kommerzielle oder gewerbliche Zwecke,
2. eine übermäßige Auslastung des Schulnetzes für private Zwecke,
3. die Integration von kommerzieller Werbung (ausgenommen die Diskussion über die Vor- und Nachteile eines Produktes durch Benutzerinnen und Benutzer) in schüler- oder lehrerbezogene Webpräsenzen sowie Lernplattformen,
4. eine Verwendung mit dem Ziel der Realisierung von illegalen Handlungen sowie der Versuch, unberechtigten Zugang zu Systemen, Software, Diensten oder Informationen zu erlangen,
5. eine Verwendung zu Zwecken der Nachrichtenübermittlung, welche die öffentliche Ordnung und Sicherheit oder die Sittlichkeit gefährdet oder gegen Gesetze verstößt,
6. eine Verwendung, die eine Belästigung oder Verängstigung anderer Benutzerinnen oder Benutzer bewirkt,
7. jegliche Verwendung, die andere Benutzerinnen oder Benutzer behindert oder das gute Funktionieren der Services des Schulnetzes stört,
8. die unberechtigte Vervielfältigung und Verteilung von Software sowie jede Art der Verwendung, die im Widerspruch zum Urheberrechtsgesetz steht.

Über die Zulässigkeit einer konkreten Verwendung hat im Zweifelsfall die Schulleitung zu entscheiden.
Die Schulleitung kann weitere standortspezifische IT-Nutzungsbedingungen anordnen. Sie kann dabei das Schulforum bzw. den Schulgemeinschaftsausschuss beratend beiziehen.

§ 13: Funktionalitäten der Endgeräte im IKT-gestützten Unterricht

1. Die im IKT-gestützten Unterricht eingesetzten IT-Systeme und Dienste haben den Videoeinsatz und die Präsentationsmöglichkeiten zu unterstützen.
2. Bei Aktivierung der Kameras sind die technischen Möglichkeiten der Schülerinnen und Schüler, der Schutz der familiären Privatsphäre in der Wohnung der Schülerinnen und Schüler sowie die besonderen Bedürfnisse von Schülerinnen und Schülern mit Behinderung nach Maßgabe der technischen Möglichkeiten zu berücksichtigen.
3. Aufzeichnungen des Unterrichts durch Video- oder Audioaufnahmen oder Screenshots sind nur mit Einwilligung aller Betroffenen gemäß Art. 7 DSGVO in Verbindung mit § 4 Abs. 4 DSG zulässig.

§ 14: Elektronische Kommunikation mit Erziehungsberechtigten

1. Sofern die Erziehungsberechtigten die Möglichkeit einer elektronischen Kommunikation mit der Schule nützen wollen, ist durch die zum Einsatz kommenden IT-Systeme und Dienste sicherzustellen, dass die elektronische Kommunikation mit den Erziehungsberechtigten der jeweiligen Schülerin bzw. des jeweiligen Schülers erfolgt und die Kenntnisnahme der Nachricht durch die Erziehungsberechtigten für die Schule nachvollziehbar ist.

§ 15: Verantwortlichkeit bei schulischen Datenverarbeitungen

Abgrenzung der datenschutzrechtlichen Verantwortlichkeit bei Datenverarbeitungen am Schulstandort

Verantwortlicher im Sinne des Art. 4 Z 7 DSGVO ist

1. hinsichtlich der Rechtmäßigkeit der Verarbeitung personenbezogener Daten und Einhaltung der Grundsätze des Art. 5 DSGVO durch die Bildungseinrichtung sowie hinsichtlich der Wahrung des Datenschutzes am Schulstandort gemäß § 4 Abs. 1 BilDokG 2020 die jeweilige Schulleitung und

2. hinsichtlich der Gewährleistung der Datensicherheit der nötigen IT-Systeme und Dienste für Datenverarbeitungen (zB einer Schulverwaltungssoftware und deren Hosting) jene Stelle, die als Maßnahme bezüglich der IT-Ausstattung an Schulen die Entscheidung darüber trifft.

§§ 10 + 11 Mobile Device Management

- Jedenfalls bei Schulverwaltung am Endgerät
- Jedenfalls bei Endgeräten im Schulnetz
- Freiwillig bei bei direkter Verwendung pädagogischer Webservices
- Rechtliche Anforderungen technologieneutral
- Bei konkreter Implementierung immer Risikoabwägung zwischen IT-Sicherheit einerseits und Datenschutz bzw Eingriff in Endgerät andererseits
- Musterlösungen, Handreichungen, Schulungen für MDM werden durch BMBWF zur Verfügung gestellt
- Andere Lösungen gemäß § 6 SchDigiG auch möglich

§ 8 Hosting (Rahmenbedingungen Cloud-Nutzung)

- Keine neue Regelung durch die VO. Es gelten die seit mehreren Jahren bewährten Rahmenbedingungen des BMBWF zum Einsatz von privaten Clouddiensteanbietern im IT-gestützten Unterricht
- NICHT für Schulverwaltung
- Nur Clouddiensteanbieter mit BMBWF-Vereinbarung (derzeit: Apple, Google, Microsoft)

§ 5 Authentifizierung (2. Faktor für Schulverwaltung)

§ 6 Bildungsstammportale (Benutzerverzeichnisse aus Schulverwaltungen für Login etc)

§ 10. Endgeräteverwaltung für digitale Endgeräte

Um die Funktionalität und Sicherheit aller digitalen Endgeräte mittels geeigneter technischer Maßnahmen, insbesondere durch Integration in eine Endgeräteverwaltung (Mobile Device Management), sicherzustellen, haben die von der Stelle gemäß § 15 Z 2 bzw. vom Dienstgeber eingesetzten Systeme zur Endgeräteverwaltung folgende technische und organisatorische Maßnahmen zu gewährleisten:

1. *automatisiertes Einspielen von Sicherheits- und Betriebssystemupdates auf den digitalen Endgeräten,*
2. *aktueller Schutz vor Schadsoftware auf digitalen Endgeräten zum Schutz des Schulnetzes,*
3. *sicherer Betrieb im Schulnetz gemäß den für die jeweilige Benutzerin oder den jeweiligen Benutzer festgelegten Zugriffsrechten,*
4. *bei Verlust die Möglichkeit zur Fernlokalisierung, Fernsperre bzw. Fernlöschung der digitalen Endgeräte bei technischer Möglichkeit auf ausdrücklichen und dokumentierten Wunsch der Geräteinhaberin oder des Geräteinhabers, soweit das Endgerät erreichbar ist, und*
5. *Aktivierung der für die Endgeräteverwaltung erforderlichen Software-Komponenten auf den verwalteten digitalen Endgeräten.*

§ 10. Endgeräteverwaltung für digitale Endgeräte

- Jedenfalls sind die Funktionen des MDM so auszugestalten, dass auf die Bereiche am Endgerät nicht über die obigen Aspekte der IT-Sicherheit (Schutz von Schadsoftware) hinausgehend zugegriffen wird, die für die persönliche Ablage von Dateien der Schüler/innen verwendet werden

- etwa: Eigene Dateien, Fotos, Browserverlauf, Chat-Inhalte und Protokolle, Bewegungsdaten etc.).

- Auch wird darauf hingewiesen, dass im Zuge der Konfiguration AGBs und sonstige Bestimmungen bewusst zu bestätigen sind.

§ 11. Anwendungsbezogene Anforderungen an dig. Endgeräte (2/3)

(1) Die Verwendung digitaler Endgeräte ist zulässig

1. *für Datenverarbeitungen gemäß § 4 Z 1 und 2, sofern die Endgeräte*
   - *a) durch den Dienstgeber als Sachbehelf gemäß § 80 BDG 1979 bzw. § 23 VBG zur Verfügung gestellt werden,*
   - *b) die vorgesehenen Methoden im Rahmen der Mehr-Faktor-Authentifizierung gemäß § 5 Abs. 2 unterstützen,*
   - *c) mit einer Endgeräteverwaltung gemäß § 10 betrieben werden bzw. durch die Betreuung der Dienstgeräte im Rahmen der Schul-IT alle Anforderungen des § 10 Z 1 bis 4 gewährleistet sind und*
   - *d) lokale Daten möglichst in verschlüsselter Form speichern und*
2. *für Datenverarbeitungen gemäß § 4 Z 3 und 4, sofern die im Schulnetz befindlichen Endgeräte mit einer Endgeräteverwaltung gemäß § 10 betrieben werden.*

(2) Wenn an einem Schulstandort die Entscheidung für die einheitliche Verwendung digitaler Endgeräte insbesondere im Rahmen eines Digitalisierungskonzepts gemäß § 2 Abs. 2 SchDigiG getroffen wurde, so ist eine Beschreibung der Gerätetypen festzulegen und sind ausschließlich Endgeräte dieser Typen zu verwenden.

§ 11: Anwendungsbezogene Anforderungen an dig. Endgeräte (3/3)

(3) Um die Speicherung personenbezogener Schülerinnen- und Schülerdaten am Endgerät zu vermeiden, sind IT-Systeme und Dienste für Datenverarbeitungen gemäß § 4 Z 1 und 2 grundsätzlich webbasiert zur Verfügung zu stellen. Stehen ausnahmsweise an Schulen keine webbasierten IT-Systeme und Dienste für die genannten Datenverarbeitungen zur Verfügung, so sind durch die jeweiligen Stellen gemäß § 15 Z 2 technische und organisatorische Maßnahmen, die eine gleichwertige IT-Sicherheit wie beim Einsatz webbasierter Lösungen gewährleisten, vorzusehen und diesbezügliche Regelungen, wie etwa Festplattenverschlüsselung, für die Verwendung festzulegen.

(4) Anstelle einer Einbindung in eine Endgeräteverwaltung gemäß § 10 können Zugriffe auf IT-Systeme und Dienste über ein schulseitig betriebene Remote Desktop Service erfolgen, sofern gewährleistet ist, dass alle Anforderungen dieser Verordnung hinsichtlich Authentifizierung, Hosting des Remote Desktop Service, organisatorischer Maßnahmen sowie eines sicheren Betriebs ohne direkte Datenhaltung am Endgerät durch die Funktionalität des Remote Desktop Services erfüllt werden.

Zeit für Fragen

Wie geht es weiter?

- Ihre Teilnahme an der PH Steiermark als Fortbildung geltend machen
- Begleitmaterial auf den Informationsportalen des NCoC eEducation Austria nutzen, Einstieg über digitaleslernen.oead.at
- Weitere regionale Unterstützungsangebote in Anspruch nehmen

Wo finden Sie Antworten auf weitere auftretende Fragen?

- FAQs des OeAD
- Im OeAD Digitales Lernen Newsletter
- Ihre Fragen werden noch nicht beantwortet?
  Schreiben Sie dem OeAD: digitaleslernen@oead.at
- Bei Fragen zur PH-online Anmeldung: medienbildung@phst.at

Vielen Dank für Ihre Aufmerksamkeit!

digitaleslernen.oead.at

digitaleslernen@oead.at

Pädagogische Hochschule Steiermark
Bundesministerium Bildung, Wissenschaft und Forschung