



Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

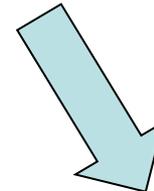
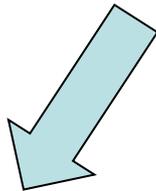
Datenschutz ...

...was ist das?

Nicht die Daten sollen geschützt werden, sondern die Person!

→ Schutz der Privatsphäre und der Persönlichkeitsrechte

Wer bedroht Persönlichkeitsrechte mehr - Staat oder Private?



Bedrohungen durch den Staat:

- Online-Durchsuchung
- Kfz-Kennzeichenerfassung
- Vorratsdatenhaltung

Bedrohung durch Private:

- kein Handy- oder Mietvertrag wegen negativer Schufa-Auskunft,
- VÜ der Mitarbeiter von Discountern (Lidl, Schlecker)
- Einsatz von Kundenkarten zwecks Erstellung von Kundenprofilen
- Informationsmacht von Google
- Implantierte Chips bei Arbeitnehmern



© Thomas Plaßmann

Quelle: <https://www.youngdata.de/datenschutz/>

Die ersten Datenschutzregeln

- Eid des Hippokrates
- Beichtgeheimnis
- Bankgeheimnis
- Sozialgeheimnis
- ...

- 1974: Rheinland-Pfalz weltweit das dritte Land, das ein eigenes Datenschutzgesetz erlassen hat
- 1977: 1. Bundesdatenschutzgesetz
- 1983: Volkszählungsurteil
- 1995: EU-Datenschutzrichtlinie
- 2018: EU-Datenschutz-Grundverordnung



- 1974: Rheinland-Pfalz weltweit das dritte Land, das ein eigenes Datenschutzgesetz erlassen hat
- 1977: 1. Bundesdatenschutzgesetz
- **1983: Volkszählungsurteil**
- 1995: EU-Datenschutzrichtlinie
- 2018: EU-Datenschutz-Grundverordnung



Öffentlichkeitssphäre

- Bereich, in dem der Einzelne sich der Öffentlichkeit bewusst zuwendet

Sozialsphäre

- Bereich, in dem sich der Mensch als soziales Wesen im Austausch mit anderen Menschen befindet (z. B. Beruf)

Privatsphäre

- Räumlich (häuslicher Bereich) und inhaltlich (Sachverhalte, die typischerweise privat bleiben)

Intimsphäre

- Innere Gedanken- und Gefühlswelt, Sexualbereich

- 1974: Rheinland-Pfalz weltweit das dritte Land, das ein eigenes Datenschutzgesetz erlassen hat
- 1977: 1. Bundesdatenschutzgesetz
- 1983: Volkszählungsurteil
- 1995: EU-Datenschutzrichtlinie
- **2018: EU-Datenschutz-Grundverordnung**



Quelle: <https://www.datenschutz.rlp.de/de/startseite/>

Wann gilt die DS-GVO nicht?

- Für natürliche Personen, die personenbezogene Daten zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten verarbeiten
- Für die Datenverarbeitung zum Zwecke der Strafverfolgung und Gefahrenabwehr durch die zuständigen Behörden

Die wichtigsten Begriffe in der DS-GVO

- Personenbezogene Daten (Art. 4 Nr. 1 DS-GVO)
- Verarbeitung (Art. 4 Nr. 2 DS-GVO)
- Verantwortlicher (Art. 4 Nr. 7 DS-GVO)
- Einwilligung der betroffenen Person (Art. 4 Nr. 11 DS-GVO)

Die wichtigsten Begriffe in der DS-GVO

➤ **Personenbezogene Daten (Art. 4 Nr. 1 DS-GVO)**

- Verarbeitung (Art. 4 Nr. 2 DS-GVO)
- Verantwortlicher (Art. 4 Nr. 7 DS-GVO)
- Einwilligung der betroffenen Person (Art. 4 Nr. 11 DS-GVO)



→ Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen („betroffene Person“)

= über eine Person etwas aussagen oder mit ihr in Verbindung zu bringen sind

→ „identifizierte“ = bestimmte/personenbezogene Information

→ „identifizierbare“ = bestimmbare/personenbeziehbare Informationen

- nicht: anonyme Daten → kein Datenschutzproblem
- Abgrenzung „anonym“ / „identifizierbar“
 - Ist die Zuordnung zu einer bestimmten Person mittels Zusatzwissen (insbesondere mittels Zuordnung zu einer Kennung, zu Standortdaten oder zu besonderen Merkmalen) möglich?
 - Bsp.: Kfz-Daten, IP-Adresse bei Internetnutzung

Die wichtigsten Begriffe in der DS-GVO

- Personenbezogene Daten (Art. 4 Nr. 1 DS-GVO)
- **Verarbeitung (Art. 4 Nr. 2 DS-GVO)**
- Verantwortlicher (Art. 4 Nr. 7 DS-GVO)
- Einwilligung der betroffenen Person (Art. 4 Nr. 11 DS-GVO)



→ Jeder mit oder ohne Hilfe automatisierter Verfahren durchgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten

Z.B.: erheben, erfassen, ordnen, speichern, verändern, auslesen, abfragen, verwenden, offenlegen durch Übermittlung, abgleichen, verknüpfen, löschen...

Die wichtigsten Begriffe in der DS-GVO

- Personenbezogene Daten (Art. 4 Nr. 1 DS-GVO)
- Verarbeitung (Art. 4 Nr. 2 DS-GVO)
- **Verantwortlicher (Art. 4 Nr. 7 DS-GVO)**
- Einwilligung der betroffenen Person (Art. 4 Nr. 11 DS-GVO)



→ Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

→ Träger oder Schule?

→ OLG Hamm, Urteil vom 9.3.2018 – I-11 U 25/17

→ Einzelne Lehrkraft als Verantwortlicher?

Die wichtigsten Begriffe in der DS-GVO

- Personenbezogene Daten (Art. 4 Nr. 1 DS-GVO)
- Verarbeitung (Art. 4 Nr. 2 DS-GVO)
- Verantwortlicher (Art. 4 Nr. 7 DS-GVO)
- **Einwilligung der betroffenen Person (Art. 4 Nr. 11 DS-GVO)**



→ Jede freiwillige für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung, in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist

Änderungen durch die DS-GVO

- Stärkere Betonung der Freiwilligkeit
 - Art. 7 Abs. 4 DS-GVO, § 20 Abs. 2 LDSG neu
 - Abhängigkeitsverhältnis, Zeitpunkt der Einwilligung, rechtlicher oder wirtschaftlicher Vorteil, gleichgelagerte Interessen zwischen Arbeitgeber und Beschäftigten
- Eindeutige bestätigende Handlung (EG 32): Untätigkeit / bereits angekreuzte Kästchen nicht ausreichend!

Anforderungen an die Einwilligung (Art. 7 DS-GVO)

- Nachweisbarkeit
 - Kein Schriftformerfordernis in DS-GVO, aber wegen Beweislast anzuraten
- Verständlich, leicht zugänglich, klare und einfache Sprache
 - Problembewusstsein innerhalb der Grenzen des Möglichen zeigen
- Widerrufsmöglichkeit!
 - Belehrung
 - Erfolgter Widerruf berührt nicht die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung

Einwilligung eines Kindes

- Anbieter eines sog. „Dienstes der Informationsgesellschaft“
 - Angebot, das einem Kind unter 16 Jahren „direkt“ gemacht wird
 - Anbieter müssen durch „angemessene Anstrengungen“ sicherstellen, dass die Einwilligung der Eltern vorliegt (Art. 8)
- Bsp.: Verwendung personenbezogener Daten von Kindern für Werbezwecke, Bildung von Profilen, Newsletter; auch soziale Netzwerke wie Facebook und WhatsApp

„Angemessene Anstrengungen“ bei WhatsApp



WhatsApp aktualisiert seine Nutzungsbedingungen und Datenschutzrichtlinie, um neue Funktionen aufzunehmen und neue gesetzliche Datenschutzregelungen der Europäischen Union zu berücksichtigen. Lies unsere [Nutzungsbedingungen](#) und [Datenschutzrichtlinie](#), welche erläutert, wie wir deine Informationen sammeln, benutzen und teilen, um WhatsApp zur Verfügung zu stellen, und wie wir mit unserem Mutterkonzern Facebook und den anderen Facebook-Unternehmen zusammenarbeiten. Erfahre auf dem nächsten Bildschirm mehr über unsere Praktiken im Umgang mit Informationen und stimme dort unseren [Nutzungsbedingungen](#) bis zum **10. Juni 2018** zu, um WhatsApp weiter benutzen zu können.

WEITER



Aktualisierte Nutzungsbedingungen und Datenschutzrichtlinie

Lies diese Seite sowie die aktualisierten Fassungen unserer [Nutzungsbedingungen](#) und [der Datenschutzrichtlinie](#). Grundlage von WhatsApp sind wirksame Vorkehrungen in Sachen Datenschutz und Datensicherheit wie etwa die [Ende-zu-Ende-Verschlüsselung](#) deiner Nachrichten und Anrufe, was bedeutet, dass weder wir noch Dritte diese lesen oder mithören können. Hier einige wichtige Punkte:

Altersanforderungen bei WhatsApp Ireland. WhatsApp Ireland Limited

Bestätige, dass du mindestens 16 Jahre alt bist

Tippe auf "Zustimmen", um unseren Nutzungsbedingungen zuzustimmen.

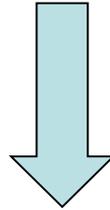
ZUSTIMMEN

zu den [Facebook-Unternehmen](#)

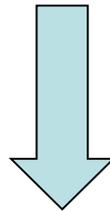
Grundsätze der Datenverarbeitung - ausgewählte Schwerpunkte

- Rechtmäßigkeit der Verarbeitung (Lawfulness)
- Verarbeitung nach Treu und Glauben (Fairness)
- Transparenz (Transparency)
- Zweckbindung (Purpose Limitation)
- Datenminimierung (Data Minimisation)
- Richtigkeit der Datenverarbeitung (Accuracy)
- Speicherbegrenzung (Storage Limitation)
- Integrität und Vertraulichkeit (Integrity and Confidentiality)

Grundregeln“ in Art. 5 Abs. 1 DSGVO



Rechenschaftspflicht für Verantwortlichen aus
Art. 5 Abs. 2 DSGVO



Umsetzung z. B. durch Verzeichnis der Verarbeitungstätigkeiten, Art. 30 DSGVO

Grundsätze der Datenverarbeitung - ausgewählte Schwerpunkte

➤ **Rechtmäßigkeit der Verarbeitung (Lawfulness)**

- Verarbeitung nach Treu und Glauben (Fairness)
- Transparenz (Transparency)
- Zweckbindung (Purpose Limitation)
- Datenminimierung (Data Minimisation)
- Richtigkeit der Datenverarbeitung (Accuracy)
- Speicherbegrenzung (Storage Limitation)
- Integrität und Vertraulichkeit (Integrity and Confidentiality)

Ausgangspunkt: Artikel 6 Abs.1 DS-GVO

- Einwilligung der betroffenen Person zu der Verarbeitung der sie betreffenden pbD für einen oder mehrere bestimmte Zwecke (lit. a)
- ...
- Verarbeitung erforderlich zur Erfüllung einer rechtlichen Verpflichtung, der Verantwortlicher unterliegt (lit. c)
- ...
- Verarbeitung ist für Aufgaben erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (lit. e)
- ...

- Legitimierende Rechtsgrundlage
- Ggf. sieht gesetzlicher Erlaubnistatbestand Verarbeitungszweck vor
 - → Verarbeitung außerhalb dieses Zwecks nicht mehr von Rechtsgrundlage gedeckt → unrechtmäßig
 - Bsp.: § 26 Bundesdatenschutzgesetz (BDSG) „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“

Gesetzliche Grundlagen im Schulbereich

Datenschutz-Grundverordnung

- Schulgesetz
- Privatschulgesetz

- Schulordnung für die öffentlichen Grundschulen
- Übergreifende Schulordnung
- Schulordnung für die öffentlichen berufsbildenden Schulen
- Schulordnung für die öffentlichen Sonderschulen

Landesdatenschutzgesetz

Schulgesetz / Schulordnung

→ Was steht da über Datenschutz drin?

- Was darf ins Klassenbuch, was nicht?
- Verbot der Weitergabe von Schülerdaten für Werbezwecke
- Nutzung privater Endgeräte („Bring your own device“)
- Datenübermittlung bei Schulwechsel
- Bild- und Tonaufzeichnungen des Unterrichts
- Datenverarbeitung bei der Schulgesundheitspflege
- Einsichtsrecht der Eltern in Schülerakte
- ...

Grundsätze der Datenverarbeitung - ausgewählte Schwerpunkte

- Rechtmäßigkeit der Verarbeitung (Lawfulness)
- Verarbeitung nach Treu und Glauben (Fairness)
- **Transparenz (Transparency)**
- Zweckbindung (Purpose Limitation)
- Datenminimierung (Data Minimisation)
- Richtigkeit der Datenverarbeitung (Accuracy)
- Speicherbegrenzung (Storage Limitation)
- Integrität und Vertraulichkeit (Integrity and Confidentiality)

- Verarbeitung nicht „hinter dem Rücken“ der betroffenen Person
- Unterrichtung des Betroffenen über Existenz des Verarbeitungsvorgangs und dessen Zwecke
- Information in leicht zugänglicher, verständlicher, klarer und einfacher Sprache
 - Hinweis auf:
 - Umfang der Verarbeitung
 - Identität des Verantwortlichen
 - Zwecke der Verarbeitung
 - Rechte der betroffenen Personen
 - Risiken der Verarbeitung
- Keine Pflicht zu kleinteiligen Informationen über jedes Detail der Verarbeitung
- Erweiterung des Auskunftsrechts der betroffenen Person (Art. 15)
- Verpflichtung zur Benachrichtigung bei Datenschutzverstößen (Art. 34)
- Veröffentlichung der Angaben zum betrieblichen oder behördlichen Datenschutzbeauftragten (Art. 37 Abs. 7)

Grundsätze der Datenverarbeitung - ausgewählte Schwerpunkte

- Rechtmäßigkeit der Verarbeitung (Lawfulness)
- Verarbeitung nach Treu und Glauben (Fairness)
- Transparenz (Transparency)
- **Zweckbindung (Purpose Limitation)**
 - Datenminimierung (Data Minimisation)
 - Richtigkeit der Datenverarbeitung (Accuracy)
 - Speicherbegrenzung (Storage Limitation)
 - Integrität und Vertraulichkeit (Integrity and Confidentiality)

- Einmal erhobene und gespeicherte Daten sollen nicht für beliebige Zwecke weiterverarbeitet werden
- Begrenzung der Verarbeitungsmöglichkeiten auf legitimen, gegenüber der betroffenen Person informierten, Zweck
- „festgelegte“ Zwecke
 - Zweckbestimmung bereits zum Zeitpunkt der Erhebung
 - Verantwortlicher muss Einhaltung des Zweckbindungsgrundsatzes nachweisen können (Art. 5 Abs. 2)
 - Dokumentation die Nachvollziehung durch Dritte zulässt → Schriftform empfehlenswert → Verarbeitungsverzeichnis
- „eindeutig“ festgelegte Zwecke
 - Hinreichende Bestimmtheit
- „Legitimität“
 - Nimmt Bezug auf Rechtmäßigkeit (Art. 5 Abs. 1 lit. a) DSGVO

- **ACHTUNG!**
 - Zweckänderung und Durchbrechung des Zweckbindungsgrundsatzes = Weiterverarbeitung!
 - Nur zulässig unter den Voraussetzungen des Art. 6 Abs. 4 DSGVO / § 7 LDSG
 - Vereinbarkeit von ursprünglichem und neuem Zweck (siehe Kriterien des Art. 6 Abs. 4)
 - Falls keine Vereinbarkeit → neue Erhebung, ansonsten Einwilligung des Betroffenen in neuen Zweck oder Rechtsgrundlage
 - Bsp.: § § 23 und 25 BDSG n. F.

Fall 1: Der Störenfried

Eine Schule in Mainz betreibt ein Schülercafé, welches sowohl von Schülern als auch von Eltern ehrenamtlich betreut wird. Schüler S, welcher auch in diesem Café aushalf, entwendete nachgewiesenermaßen Geld aus der Kasse und erhielt daraufhin Hausverbot. Um den Eltern, welche nicht alle Schüler der Schule persönlich kennen, zu ermöglichen, S zu identifizieren und das Hausverbot durchzusetzen, bringt die Schule das Schülersausweisfoto des S unter dem Tresen mit einem entsprechenden Hinweis auf das Hausverbot an.

Ist dieses Vorgehen zulässig?



Quelle:
<https://pixabay.com/illustrations/stop-challenge-showing-sign-3077813/>

Grundsätze der Datenverarbeitung - ausgewählte Schwerpunkte

- Rechtmäßigkeit der Verarbeitung (Lawfulness)
- Verarbeitung nach Treu und Glauben (Fairness)
- Transparenz (Transparency)
- Zweckbindung (Purpose Limitation)
- Datenminimierung (Data Minimisation)
- Richtigkeit der Datenverarbeitung (Accuracy)
- **Speicherbegrenzung (Storage Limitation)**
- Integrität und Vertraulichkeit (Integrity and Confidentiality)

- Konkretisierung des Zweckbindungsgrundsatzes in zeitlicher Hinsicht
- Daten müssen derart geändert werden, dass Identifizierung der betroffenen Person nicht mehr möglich ist
- „Recht auf Vergessenwerden“ aus Art. 17 Abs. 1 DSGVO
- Aber: Ausnahmen des Abs. 3
 - Hier insbesondere Erfüllung einer rechtlichen Verpflichtung (Art. 17 Abs. 3 lit. b))
 - Bsp.: steuerrechtliche Aufbewahrungspflichten
- Vorgesehene Löschfristen auch Teil des Verarbeitungsverzeichnisses (Art. 35)

Grundsätze der Datenverarbeitung - ausgewählte Schwerpunkte

- Rechtmäßigkeit der Verarbeitung (Lawfulness)
- Verarbeitung nach Treu und Glauben (Fairness)
- Transparenz (Transparency)
- Zweckbindung (Purpose Limitation)
- Datenminimierung (Data Minimisation)
- Richtigkeit der Datenverarbeitung (Accuracy)
- Speicherbegrenzung (Storage Limitation)
- **Integrität und Vertraulichkeit (Integrity and Confidentiality)**

- Geeignete technische und organisatorische Maßnahmen
 - Konkretisiert in Art. 32 DSGVO
 - Erforderliche Maßnahmen abhängig von Risiko eines unberechtigten Zugriffs, Art der Verarbeitung, Bedeutung der Daten für Rechte und Interessen der betroffenen Person
 - Bsp.: persönliche Finanz- und Gesundheitsdaten schutzbedürftiger als Name oder Alter
 - Umsetzung der internen Vorgaben und des Sicherheitskonzepts
 - Anweisungen des Verantwortlichen und des Datenschutzbeauftragten folgen

Datenpanne! Was nun?

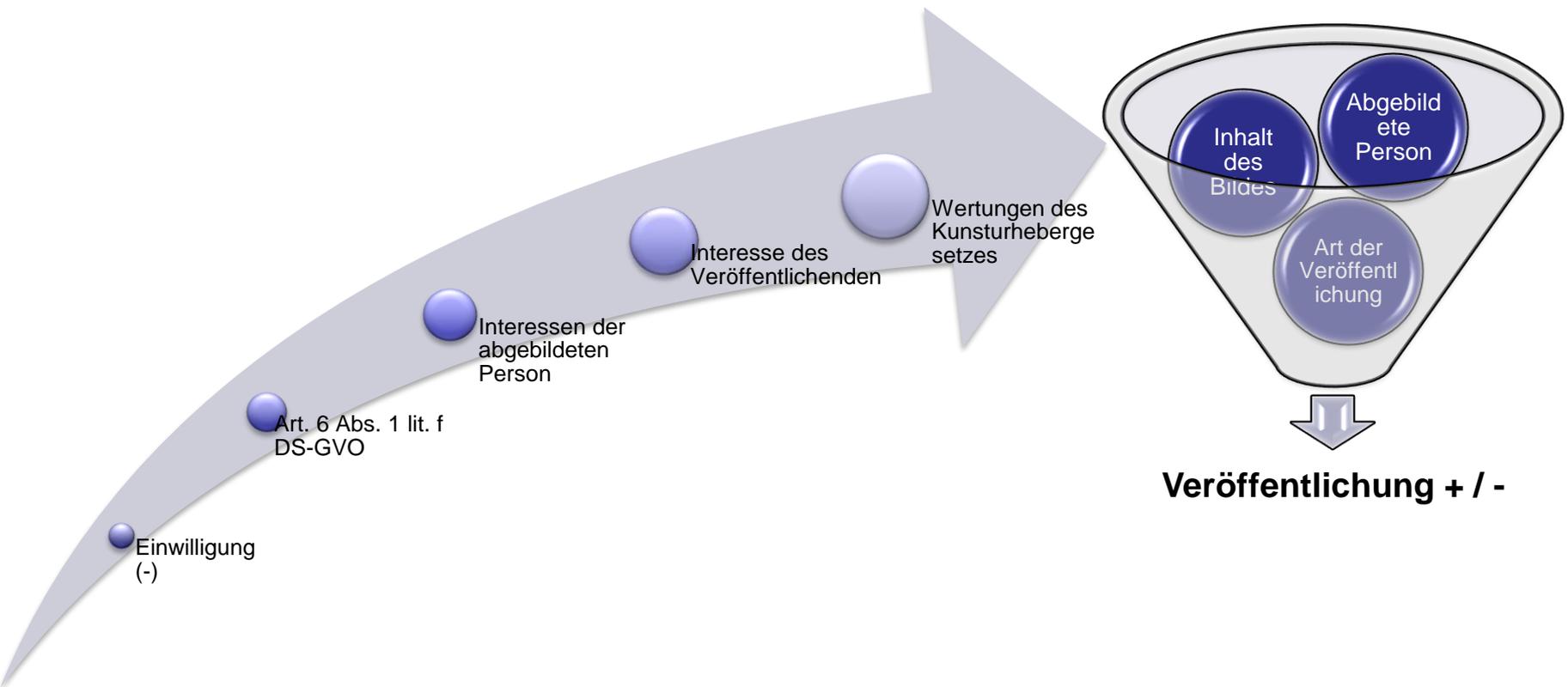
Wenn mal etwas schiefgeht...

Maßnahmen nach Datenpanne

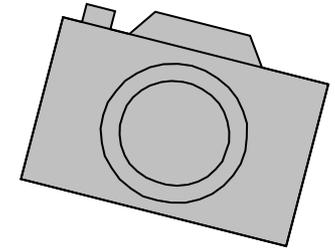
- Meldung an die Aufsichtsbehörde innerhalb 72 Stunden nach Bekanntwerden, es sei denn Verletzung führt voraussichtlich nicht zu Risiko für Rechte und Freiheiten natürlicher Personen
- Inhalt der Meldung gem. Art. 33 Abs. 3 DSGVO
 - Art der Verletzung, mit Angabe der Kategorie und der ungefähren Zahl der betroffenen Personen
 - Kontaktdaten des DSB
 - Beschreibung der wahrscheinlichen Folgen
 - Ergriffene Maßnahmen zur Behebung der Verletzung
- Ggf. Benachrichtigung der betroffenen Person gem. Art. 34 DSGVO

Recht am eigenen Bild

- Rechtsgrundlage erforderlich für Anfertigung UND Veröffentlichung
 - Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO)
 - Anderer Tatbestand des Art. 6 Abs. 1 lit. b – f DS-GVO



Wertungen der § § 22, 23 Kunsturhebergesetz (KUG)



- Eingriff in das allgemeine Persönlichkeitsrecht (Recht am eigenen Bild)
- Ist grundsätzlich nur mit Einwilligung des Abgebildeten zulässig! Widerruf möglich
- Keine konkludente Einwilligung durch Posieren vor der Kamera
- Veröffentlichung liegt vor, auch wenn der Abgebildete nur durch eingeschränkten Personenkreis identifiziert werden kann
- Ausnahme (Einwilligung nicht erforderlich) bei
 - Veranstaltungen
 - Person ist nur „Beiwerk“
 - Personen der Zeitgeschichte („Prominente“)
- Verstoß = Straftatbestand (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe); aber Antrag erforderlich

Fall 2: Der Sitzplan

Lehrerin L macht zu Beginn des neuen Schuljahres mit ihrem Mobiltelefon Portraitfotos von Schülerinnen und Schülern ihrer neuen Klassen als Gedächtnisstütze und zur Vervollständigung des Sitzplans. Als sich Schüler J weigert, droht L mit einem Klassenbucheintrag. Wie beurteilen Sie das Vorgehen von L?



Quelle: <https://pixabay.com/photos/lecture-school-university-meeting-2044621/>

Fall 3: Im Sportunterricht

Sportlehrerin S vergibt ihre Noten gerne besonders gründlich. Damit ihr bei den zu benotenden Übungen der Schüler am Barren kein Detail entgeht, zeichnet sie diese mittels Videokamera auf, um sie sich daheim in Ruhe und bei Bedarf mehrmals anschauen zu können.

Zulässig?



Quelle: <https://pixabay.com/illustrations/white-male-3d-man-isolated-3d-1871430/>

Veröffentlichung von heimlich gefertigten Unterrichtsmitschnitten

- Erzieherische Einwirkung (z. B. zeitweise Wegnahme des Handys) oder, falls erforderlich, Schulordnungsmaßnahmen ergreifen
- Zivilrechtliche Unterlassungs- und Beseitigungsansprüche gegenüber SchülerIn bzw. Eltern und Betreiber der Internetseite geltend machen (Meldebutton des Portals nutzen)
- „Recht auf Vergessenwerden“ gegenüber Google geltend machen. Je nach Schwere des Verstoßes Möglichkeiten des Strafrechts prüfen (Strafmündigkeit ab 14 J.).
- In Frage kommende Straftatbestände:
 - § 201 StGB verbietet unbefugte Aufnahme des nicht öffentlich gesprochenen Wortes
 - § § 22, 23, 33 Kunsturhebergesetz verbietet Veröffentlichung von Bildnissen ohne Einwilligung („Recht am eigenen Bild“)

Bring your own device (BYOD)

Rechtsgrundlage: § 89 Abs. 4 ÜSchulO

- Genehmigung der Schulleitung
- Einverständnis der Lehrkraft bez. Kontrolle des Gerätes



Technisch-organisatorische Maßnahmen, um
Gerät gegen Zugriff Unbefugter abzusichern



Fall 4: Die schnelle Kommunikation

Stellen Sie sich vor, Sie seien der Datenschutzbeauftragte der Schule, an der Sie lehren.

Ein Kollege kommt mit folgender Fragestellung auf Sie zu:
„Ist es erlaubt, als Lehrer WhatsApp zur Kommunikation mit Schülern, Eltern oder auch Kollegen zu nutzen?“

Was antworten Sie ihm?



Quelle: <https://pixabay.com/illustrations/gdpr-data-protection-privacy-3438462/>

Nutzung von Messengerdiensten

Erlaubt:

Europäische Anbieter,
die Ende-zu-Ende-
Verschlüsselung
anbieten

Bsp.: Pidgin/OTR,
SIMSme, Chiffry,
Wire, Threema

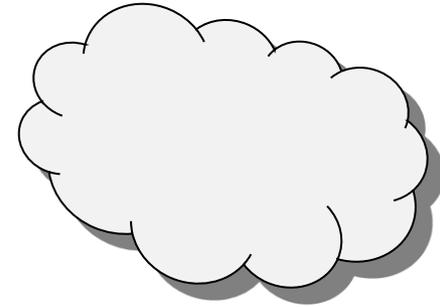
→ Distanzgebot beachten!

Nicht erlaubt:

Facebook, WhatsApp,
iMessage

Zur schulischen Kommunikation
zwischen Lehrkräften und SchülerInnen:
landeseigene, kostenfreie, auf Moodle
basierende Lernplattform
<http://lernenonline.bildung-rp.de>
→ Datensicherheit durch Verwendung
eines landeseigenen Servers

Nutzung von cloudbasierter Software zu Unterrichtszwecken

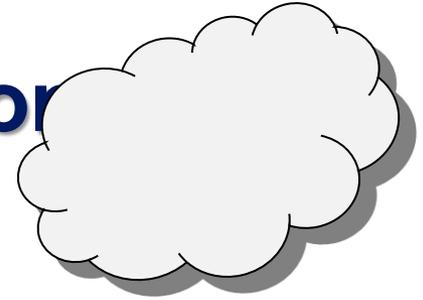


Bsp.: MS-Office 365, Google Classroom

Problem: US-amerikanische Anbieter!

- Daten werden auf Servern verarbeitet, die in rechtlicher und technischer Hinsicht nicht den europäischen Datenschutz-Standards entsprechen
- Einsatz nur dann zulässig, wenn
 - über ein Treuhandmodell der Zugriff durch US-amerikanische Stellen ausgeschlossen ist
 - keine personenbezogenen Daten in der Cloud gespeichert werden

Kommunikation mithilfe von Clouddiensten



- Nur durch öffentlich-rechtliche Cloudanbieter
- schulinterne Cloudlösungen
 - kommunale Datenzentralen
 - Landesbetrieb Daten und Information
 - Pädagogisches Landesinstitut
 - private Cloudanbieter mit Sitz innerhalb der EU
- Nicht erlaubt: Verwendung außereuropäischer Anbieter
- Dropbox
 - Microsoft OneDrive
 - Google Drive
 - iCloud kommt

Schulcampus RLP:

<https://schulcampus.bildung-rp.de>
Virtueller Campus RLP (z. B. „seafile“ als Dropbox-Alternative für Hochschulen: <https://seafile.rlp.net/>)

Möglichkeit für sicheren Datenaustausch zwischen Lehrkräften: BSCW-Server des Pädagogischen Landesinstituts
<http://bildungsnetz.bildung-rp.de/groupware.html>

Link-Liste zum Nachschlagen Bereich „Schulischer Datenschutz“

Suchanfrage Nur in Medienkompetenz suchen

BILDUNGSSERVER
Medien Kompetenz
macht Schule

AKTUELLES
10-PUNKTE-PROGRAMM
SCHULEN
MATERIALIEN
ECDL-Lernpakete
Master tool
Medienkonzepte
Tablets
Unterricht
Jugendmedienschutz
Schule, Medien, Recht
Links und Materialien zum Datenschutz
PROJEKTE
VERANSTALTUNGEN
REFERAT MEDIENKOMPETENZ
Startseite
An-/Abmelden
Impressum
Datenschutzzerklärung
Sitemap

Bildungsserver > Medienkompetenz > Materialien > Schule, Medien, Recht > Links und Materialien zum Datenschutz...

Hier erhalten Sie Links und weiterführende Informationen zum Thema Datenschutz.

Die aufgeführten Musterschreiben, Merkblätter und Materialien beziehen sich speziell auf die am häufigsten nachgefragten Bereiche zum schulischen Datenschutz und orientieren sich an den Richtlinien der Datenschutz-Grundverordnung (kurz: DS-GVO).

Mustertexte zum schulischen Datenschutz

- Private Endgeräte von Lehrkräften - Musterdatenschutzzerklärung vom Juli 2018 (neue Vorlage)
- Musterschreiben Fotos
- Elterninformationen nach Datenschutz-Grundverordnung (DS-GVO)
- Muster DS-GVO Verarbeitungsverzeichnis Verantwortlicher
- Muster DS-GVO Verarbeitungsverzeichnis Auftragsverarbeiter
- Selbstverpflichtungserklärung/Nutzungsverordnung der IT- und Kommunikationstechnik an Schulen (ohne private Nutzung)
- Selbstverpflichtungserklärung/Nutzungsverordnung der IT- und Kommunikationstechnik an Schulen (mit privater Nutzung)
- Musterschreiben Homepage DS-GVO

Merkblätter zum schulischen Datenschutz

- Datenschutzmerkblatt
- Soziale Netzwerke
- Datenschutz-Grundverordnung und Schule
- Hinweise für schulische Datenschutzbeauftragte

Materialien zum schulischen Datenschutz

- Lehrerflyer zum schulischen Datenschutz
- Informationen zu Datenschutz und Schule
- Material zur Datenschutz-Grundverordnung
- Orientierungshilfe Lernplattformen



Materialien



Nachfolgend finden Sie eine Liste von Orientierungshilfen, Arbeitspapieren, Leitlinien und Empfehlungen zu verschiedenen Bereichen. Die Materialien sind alphabetisch nach dem jeweiligen Schlagwort sortiert.

Weitere Materialien finden Sie in der

- [Infothek](#) sowie unter
- [Publikationen](#)
- [Rechtsgrundlagen](#)
- [Gerichtsentscheidungen](#)
- [Tätigkeitsberichte](#)
- [Entschlüsseungen](#) der Datenschutzkonferenz und den
- [Entschlüsseungen](#) der Konferenz der Informationsfreiheitsbeauftragten



ÜBER UNS

BÜRGERINNEN / BÜRGER

WIRTSCHAFT

VERWALTUNG

SERVICE

× Verwaltung

Datenschutz

Informationsfreiheit

Beratung

Behördliche Datenschutzbeauftragte

Datenschutzregister / Verfahrensverzeichnis

Meldung einer Datenpanne nach §18a LDSG

Themen A-Z



Nachfolgend finden Sie eine Liste von Orientierungshilfen, Arbeitspapieren, Leitlinien und Empfehlungen zu verschiedenen Bereichen. Die Materialien sind alphabetisch nach dem jeweiligen Schlagwort sortiert.

Weitere Materialien finden Sie in der

- [Infothek](#) sowie unter
- [Publikationen](#)
- [Rechtsgrundlagen](#)
- [Gerichtsentscheidungen](#)
- [Tätigkeitsberichte](#)
- [Entschliefungen](#) der Datenschutzkonferenz und den
- [Entschliefungen](#) der Konferenz der Informationsfreiheitsbeauftragten

Themenfelder

Leben digital	Informationsfreiheit	Wirtschaft	Europa
Internationales	Beschäftigtendaten- schutz	Gesundheit	Sicherheit
Medienbildung/Schule		Verwaltung digital	Open Data
Finanzen	Hochschulen/Forschung	Kommunales	Soziales

**DATENSCHUTZ**

© Syda Productions / shutterstock.com

Schule/Medienkompetenz

Seit mehreren Jahren sieht der LfDI eine seiner Hauptaufgaben in der digitalen Aufklärung und darin, den Datenschutz auch als Bildungsaufgabe zu verstehen und wahrzunehmen.

DATENSCHUTZ**Datenschutz in der Schule - Fragen und Antworten für Lehrkräfte**

Antworten zu häufig gestellten Fragen.

DATENSCHUTZ

© geralt / pixabay.com

Umsetzung der Datenschutz-Grundverordnung in den Schulen

Welcher konkrete Handlungsbedarf ergibt sich für Schulen aufgrund der EU-Datenschutz-Grundverordnung ?

MEDIENKOMPETENZ**Schülerworkshops**

Seit 2010 führt der LfDI Schülerworkshops in ganz Rheinland-Pfalz durch, um Kinder und Jugendliche ab der vierten Klasse für einen sparsamen Umgang mit ihren Daten im Netz und mögliche Gefahren bei der alltäglichen Nutzung von Smartphone, Tablet und Co. zu

DATENSCHUTZ

© Sergey Novikov / shutterstock

Datenschutz in Kitas

Ein Praxisleitfaden für Kitas in öffentlicher Trägerschaft

DATENSCHUTZ

© LfDI/pixabay.de

Veröffentlichung von Fotos auf der Homepage von Schulen oder Kindertagesstätten

Wiederholt fragen Kindertagesstätten oder Schulen beim LfDI an, ob und unter welchen Voraussetzungen Fotos oder Videos von Kindern, Lehrkräften oder Erzieherinnen und Erziehern auf der eigenen Homepage veröffentlicht werden dürfen. Bei der Beantwortung dieser Frage sind neben spezialgesetzlichen Regelungen insbesondere die Bestimmungen des Kunsturhebergesetzes zu beachten.

DATENSCHUTZ

© WerbeFabrik / pixabay.de

Videoüberwachung an Schulen

Sachbeschädigungen und Diebstähle gehören heute leider zu Schulalltag. Eine Videoüberwachung wird daher häufig als Mittel angesehen, um potenzielle Täter abzuschrecken oder Straftaten besser aufzuklären zu können. Das ist nicht ausgeschlossen, hat aber Voraussetzungen.

DATENSCHUTZ**Youngdata**

Der LfDI hat sein Internetangebot im November 2013 um eine spezielle Jugendhomepage für den Datenschutz ergänzt. Sie enthält Informationen zum Selbstschutz bei der Nutzung von Facebook, WhatsApp, Youtube, Spielkonsolen, Smartphones und anderen Anwendungen, klärt über die Gefahren von Cybermobbing auf und bietet Hintergrundinformationen zum Datenschutz im Allgemeinen.

Startseite | Datenschutzerklärung | Kontakt | Impressum

Was gibt's in deiner Nähe? News Datenschutz Digitale Selbstverteidigung Internet Facebook Google WhatsApp, Skype & Co Konsolen Smartphones Cybermobbing Staat und Bürgerdaten Videoüberwachung Informationsfreiheit Quiz

Startseite >> Was gibt's in deiner Nähe? >> Rheinland-Pfalz >> Schuldatenschutz in Rheinland-Pfalz

Schuldatenschutz in Rheinland-Pfalz

In der Schule werden sehr viele verschiedene personenbezogene Daten verarbeitet. Betroffen hiervon sind die Schülerinnen und Schüler, Eltern, Lehrkräfte sowie andere Mitarbeiterinnen und Mitarbeiter der Schule (z.B. Sekretärin, Hausmeister). Neben den eigentlichen Informationen zur Person, wie z.B. Name, Geburtsdatum, Konfession fallen darunter auch Angaben, die die Leistung und das Verhalten der Schüler umschreiben. Auch Informationen über die familiären Verhältnisse der Schülerinnen und Schüler gehören dazu. Beispielhaft sind folgende Bereiche zu nennen:

- Schulaufnahme (Anmeldeformulare; ärztliche Untersuchungen, sonderpädagogischer Förderbedarf, etc.)
- Leistungsnachweise und Leistungsbewertungen (Klassenarbeiten, Noten, Prüfungsergebnisse)
- Verhaltensbeschreibungen (z.B. anlässlich schulischer Ordnungsmaßnahmen)
- Gestaltung einer Schulhomepage
- Datenverarbeitung im Zusammenhang mit der Schulbuchausleihe, der Schülerbeförderung, der Herausgabe von Schülerzeitungen, der Arbeit von Schüler- und Elternvertretungen.

Die Verarbeitung erfolgt nicht nur in Papierform, sondern überwiegend automatisiert. Fast jede Schule setzt heute ein Schulverwaltungsprogramm zur Verwaltung personenbezogener Daten ein.

Quelle: LfDI



Schulischer Datenschutz

Fragen und Antworten für Lehrkräfte in Rheinland-Pfalz



Ein Praxisleitfaden

Handbuch „Schule.Medien.Recht.“
Hrsg: Ministerium für Bildung, Wissenschaft, Jugend und Kultur Rheinland-Pfalz; Baustein 2.7 „Datenschutzrechtliche Anforderungen bei der Verwendung von Facebook im Schulbereich“
[Download als PDF](#)

Merkblatt „Lehrkräfte und Soziale



Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Dominique Braun

Referentin

beim Landesbeauftragten für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

Postanschrift: Postfach 30 40
55020 Mainz

Büroanschrift: Hintere Bleiche 34
55116 Mainz

Telefon: +49 (6131) 208-2589
Telefax: +49 (6131) 208-2497

E-Mail: d.braun@datenschutz.rlp.de

Web: www.datenschutz.rlp.de