Rechtsinformatikzentrum
Thomas Hofer, Akad. Direktor

Die EU-Datenschutz-Grundverordnung aus Hochschulsicht

Nur ein netter Papiertiger?

Was bleibt – was ändert sich – was ist schon heute zu tun?

Referent

- Studium Rechtswissenschaften (Univ. Würzburg), 2. Jur. Staatsexamen
- Akademischer Direktor und Leiter des Rechtsinformatikzentrums der Ludwig-Maximilians-Universität München

Daneben:

- Dozent für IT-Compliance- und Informationssicherheitsrecht des Bay. IT-Sicherheitsclusters und der Bayerischen Verwaltungsschule (BVS)
- IT-Security-Beauftragter (TÜV PersCert) und Compliance-Manager

Ziele und Angebote:

- Anforderungen des Rechts in die Sprache der Anwender „übersetzen“
- Geschäftsführung, Amtsleitung, IT-Verantwortliche in KMU und Behörden für (Haftungs-)risiken sensibilisieren
- Kooperationen bei Umsetzung geforderter Maßnahmen und Konzepte

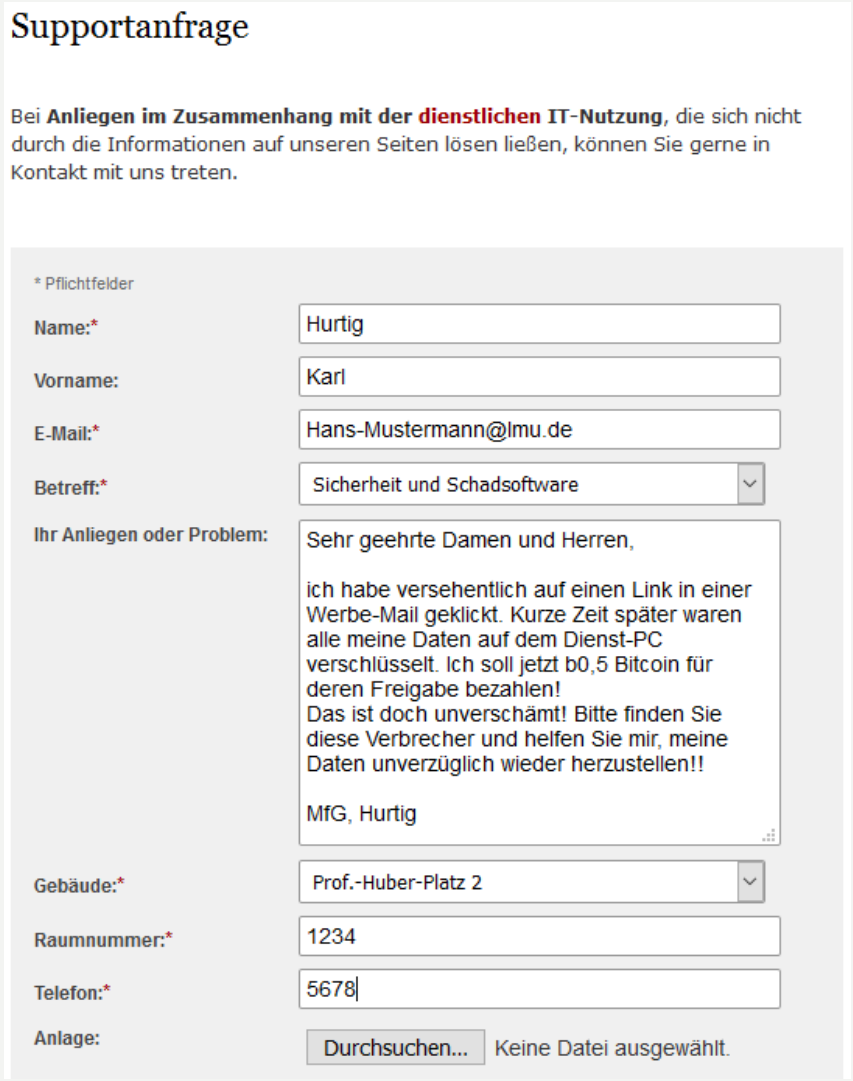
Agenda

Was Hochschulleitung und Fachverantwortliche wissen müssen…

- *Die Ausgangslage im Datenschutz*
- *Das neue Datenschutzrecht für Europa:*
  - *Was bleibt?*
  - *Was ändert sich?*
  - *Was ist ganz neu?*
- *Wie bereite ich meine Organisation auf das neue Recht vor?*

Szenario 1 - Web-Dienste

- Die Fakultät F der Hochschule L bietet auf Ihrer Website Basis-Interaktionen wie Kontaktformular und eine Online-Anmeldung zu Veranstaltungen an.
- F hat geringe Ressourcen für Pflege und Betrieb der Webdienste und Systeme. Deren Betreuung liegt seit Jahren in Personalunion bei Mitarbeiter R, der durch die laufende Aufgabenverdichtung völlig überlastet ist.
- R ist mit dem Patchen in Rückstand. Über eine bekannte Sicherheitslücke verschaffen sich Angreifer Zugriff auf die Datenbank mit den Kontaktanfragen bei F.



Supportanfrage

Bei **Anliegen im Zusammenhang mit der dienstlichen IT-Nutzung**, die sich nicht durch die Informationen auf unseren Seiten lösen ließen, können Sie gerne in Kontakt mit uns treten.

* Pflichtfelder

Name:* Hurtig

Vorname: Karl

E-Mail:* Hans-Mustermann@lmu.de

Betreff:* Sicherheit und Schadsoftware

Ihr Anliegen oder Problem:

Sehr geehrte Damen und Herren,

ich habe versehentlich auf einen Link in einer Werbe-Mail geklickt. Kurze Zeit später waren alle meine Daten auf dem Dienst-PC verschlüsselt. Ich soll jetzt b0,5 Bitcoin für deren Freigabe bezahlen!
Das ist doch unverschämt! Bitte finden Sie diese Verbrecher und helfen Sie mir, meine Daten unverzüglich wieder herzustellen!!

MfG, Hurtig

Gebäude:* Prof.-Huber-Platz 2

Raumnummer:* 1234

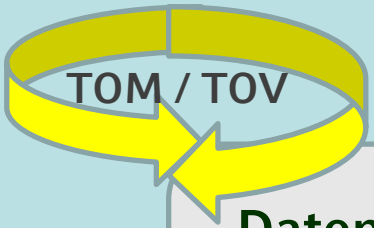
Telefon:* 5678

Anlage: Durchsuchen... Keine Datei ausgewählt.

Ausgangslage

Informationssicherheit

Schutzgut: alle relevanten Arten von Informationen jeglicher Art und Herkunft; Hard- und Software
Risiko: Verlust, Zerstörung, Vertraulichkeit, Missbrauch



Datenschutz

Schutzgut: pers.bezogene und pers.beziehbare Daten
Risiko: Verletzung von Persönlichkeitsrechten

Ausgangslage

Art. 1 Bay.DSG:

„Zweck dieses Gesetzes ist es, die Einzelnen davor zu schützen, dass sie bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch öffentliche Stellen in unzulässiger Weise in ihrem Persönlichkeitsrecht beeinträchtigt werden.“

Art. 1 DSGVO Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum ***Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten*** *und zum freien Verkehr solcher Daten.*

(2) Diese Verordnung ***schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten***

- Der Schutz der Persönlichkeit und der Privatsphäre sind Grundrechte (allgemeines Persönlichkeitsrecht, Art. 1 und Art. 2 GG, *Artikel 8 Abs. 1 der Charta der Grundrechte der Europäischen Union*)
- **Recht auf informationelle Selbstbestimmung (BVerfG, Volkszählung):** Geschützt wird die Freiheit, selbst über Verwendung und Preisgabe zu entscheiden (Wer weiß was wann und bei welcher Gelegenheit über mich?)

Ausgangslage

- Wir hinterlassen **digitale Spuren**:
  - Bewegungs-/Standortdaten (GPS)
  - Einkäufe (Bonussysteme, Karten, …)
  - Aktivität und Gesundheit (Fitness-Tracker, SmartWatch, …)
  - Dateien und E-Mails (verschiedene Cloud-Dienste, …), …
- Viele der gesammelten Daten sind für den Betrieb der Dienste nötig oder machen deren Nutzung angenehm, z.B. Cloud-Dienste
- Problem: **Korrelation der Daten („Big Data“)**
- Wer hat die Möglichkeiten dazu?
  - Große IT-Firmen wie Facebook, Google, Microsoft, Apple …
  - Internet-und Mobilfunknetzanbieter
  - Nachrichtendienste, Polizei, **Behörden**
- **These: Alles, was digitalisiert werden, wird digitalisiert werden. Mit Verspätung auch bei Behörden, Kommunen („e-Government“)**
- ***Wird dabei alles schiefgehen, was schiefgehen kann („Murphy“)?***

Zielsetzung EU-Datenschutzgrundverordnung (DSGVO)

Erwägungsgrund 9 der DS-GVO

„Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert eine Stärkung und Präzisierung der Rechte“

Stärkung und Präzisierung der Rechte der betroffenen Personen

Sowie eine

Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden.

aber ebenso **gleiche Befugnisse der Mitgliedstaaten bei der Überwachung** und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie **gleiche Sanktionen im Falle ihrer Verletzung**.“

Was ist (wirklich) neu in der DSGVO?

- **Mehr Rechte für Datensubjekte** (Recht auf „Vergessenwerden“, Recht auf Datenübertragbarkeit, Reaktionsfrist auf Anfragen)
- **Dokumentations- / Nachweispflichten** („accountability“)
- **Informationspflichten:** Organisationen müssen umfassender als bislang darüber informieren, ob und wie sie pb Daten verarbeiten
- Datenschutz durch **Technikgestaltung**
- **Risikobasierter Ansatz** nach **„Stand der Technik“**
- **Verschärfte Meldepflicht** bei Schutzverletzungen
- **Geldbußen** von bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes
- **Marktortprinzip**: Geltung nicht nur für Unternehmen innerhalb der EU, sondern auch für Unternehmen in aller Welt, die ihre Waren und Dienstleistungen EU-Bürgern anbieten.
- ….

- Zu berücksichtigende **Anforderungen** (Auszug):
  - **Neue Institute / Art. 5: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
  - Art. 6: Einwilligung oder gesetzliche Grundlage
  - Art. 8: Einwilligung von Minderjährigen
  - Art. 9: Verarbeitung besonderer Kategorien pb Daten
  - Art. 28: Auftragsdatenverarbeitung
  - Art. 30: Verzeichnis der Verarbeitungsaktivitäten
  - **Art. 32: Informationssicherheit**
  - **Art. 33, 34: Data Breach Notification (Meldepflicht)**
  - Art. 37: Datenschutzbeauftragter
- **Rechte** (Auszug):
  - **Art. 17: Recht auf Löschung („Vergessenwerden“)**
  - Art. 18: Recht auf Datenübertragbarkeit („Datenmitnahme“)
  - **Art. 25: Datenschutz durch Technik („Privacy by design“)**

Amtsblatt **L 119**

der Europäischen Union

99 Artikel und 173 Erwägungsgründe

Ausgabe in deutscher Sprache Rechtsvorschriften **59. Jahrgang**
4. Mai 2016

Inhalt *I Gesetzgebungsakte* Seite

VERORDNUNGEN

EU-Datenschutzgrundverordnung (DSGVO)

- neue, **europaweit einheitliche Rechtsgrundlage** für den Datenschutz
- großer Schritt in der Aktualisierung des europäischen Datenschutzrechts
- **gilt ab dem 25. Mai 2018** unterschiedslos für jede öffentliche und nicht-öffentliche Stelle
- Bestehendes (widersprechendes) Datenschutzrecht tritt dann automatisch außer Kraft
- **URL (UmsetzungsRestLaufzeit): 176 Tage (= ca. 25 Wochen)**
  - Abzüglich: Wochenende, Feier-, Krankheits-, Geburtstage, Fortbildungen, ...
  - Also: **nicht mehr ganz so viel Zeit!**

EU-Datenschutzgrundverordnung (DSGVO)

- enthält einige sogenannte **Öffnungsklauseln**
  = Regelungsspielräume für Konkretisierungen, Ergänzungen oder Abweichungen von den Bestimmungen der DSGVO im nationalen Datenschutzrecht
- Umsetzung der Öffnungsklauseln durch **Neufassung des BayDSG** sowie durch Änderungen im Fachrecht
- Ziel: einheitlicher Rechtsrahmen für alle öffentlichen Stellen gleichermaßen
- aber Regelungen im **BayDSG in Zukunft nur noch ergänzend** neben die Regelungen der DSGV

Gesetzentwurf

der Staatsregierung

Bayerisches Datenschutzgesetz

A) Problem

Rasche technologische Entwicklungen und die Globalisierung haben das Datenschutzrecht vor neue Herausforderungen gestellt. Die mit diesem technologischen Wandel verbundenen Risiken für den Einzelnen machen einen kohärenten und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union erforderlich.

Um eine weitergehende europäische Rechtsharmonisierung im Datenschutzrecht zu erreichen, haben sich der Rat der Europäischen Union, das Europäische Parlament und die Europäische Kommission auf eine umfassende Reform des europäischen Datenschutzrechts verständigt. Nach intensiven Verhandlungen ist am 25. Mai 2016 die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGV), (ABl. Nr. L 119 vom 4. Mai 2016, S. 1; L 314 vom 22. November 2016, S. 72) in Kraft getreten. Diese gilt gemäß Art. 99 Abs. 2 DSGV ab 25. Mai 2018 unmittelbar europaweit und löst die geltende EG-Datenschutzrichtlinie (RL 95/46/EG) ab. Neben der Gewährleistung eines freien Datenverkehrs innerhalb des Europäischen Binnenmarktes zielt die DSGV auf die Sicherstellung des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 und 3 DSGV). Materielle Regelungen und deren Anwendung durch die nationalen Behörden und Gerichte sollen durch die DSGV stärker als früher vereinheitlicht werden. Zugleich stärkt die DSGV die Rechte der Betroffenen.

Die Verabschiedung der DSGV führt zu grundlegenden strukturellen Änderungen im nationalen Datenschutzrecht: Auf Grund des Rechtsformwechsels hin zu einer Verordnung bedürfen die Reglungen in der DSGV keiner Umsetzung in das nationale Recht, sondern sind vielmehr ab 25. Mai 2018 europaweit unmittelbar anwendbar. Trotz ihres Charakters als Verordnung enthält die DSGV eine Reihe obligatorischer Handlungsaufträge an die Mitgliedstaaten, die eine zwingende Ausgestaltung im nationalen Datenschutzrecht erforderlich machen wie beispielsweise die Errichtung unabhängiger Aufsichtsbehörden. Darüber hinaus räumt die DSGV dem nationalen Gesetzgeber insbesondere im öffentlichen Bereich im Rahmen sog. Öffnungsklauseln Regelungsspielräume ein. Diese lassen Raum

Entwurf BayDSG, Stand: 28.09.2017

Art. 2

Anwendung der Verordnung (EU) 2016/679

[1]Für die Verarbeitung personenbezogener Daten durch öffentliche Stellen gelten vorbehaltlich anderweitiger Regelungen die Vorschriften der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGV) auch außerhalb des sachlichen Anwendungsbereichs des Art. 2 Abs. 1 und 2 DSGV. [2]Die Art. 30, 35 und 36 DSGV gelten nur, soweit die Verarbeitung automatisiert erfolgt oder die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Entwurf BayDSG, Stand: 28.09.2017

Anhörung der Verbände kürzlich abgeschlossen

- Weiterhin **keine (relevanten) Bußgelder gegen Behörden**

Art. 22

Geldbußen

(zu Art. 83 DSGV)

Gegen öffentliche Stellen im Sinne des Art. 1 Abs. 1 und 2 dürfen Geldbußen nach Art. 83 DSGV nur verhängt werden, soweit diese als Unternehmen am Wettbewerb teilnehmen.

Art. 23

Ordnungswidrigkeiten, Strafvorschrift

(zu Art. 84 DSGV)

(1) Mit Geldbuße bis zu dreißigtausend Euro kann belegt werden, wer geschützte personenbezogene Daten, die nicht offenkundig sind,

1. unbefugt
   a) speichert, verändert oder übermittelt,
   b) zum Abruf mittels automatisierten Verfahrens bereithält oder
   c) abruft oder sich oder einem anderen aus Dateien verschafft oder
2. durch unrichtige Angaben erschleicht.

(2) [1]Wer eine der in Abs. 1 bezeichneten Handlungen gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. [2]Die Tat wird nur auf Antrag verfolgt. [3]Antragsberechtigt sind die betroffene Person, der Verantwortliche, der Auftragsverarbeiter und die Aufsichtsbehörde.

(3) Gegen öffentliche Stellen im Sinne des Art. 1 Abs. 1 und 2 werden keine Geldbußen nach Abs. 1 verhängt.

(4) Eine Unterrichtung nach Art. 33 oder Art. 34 DSGV darf in einem Straf- oder Ordnungswidrigkeitenverfahren gegen den Verantwortlichen oder einen seiner in § 52 Abs. 1 StPO bezeichneten Angehörigen nur mit seiner Zustimmung verwendet werden.

Wenn etwas neu ist,

…ist es für alle neu?!

…Institutionen, Begriffe, Definitionen, Auslegungen

- gilt selbst für bereits im BDSG / BayDSG verwendete Begriffe), daher Augenmerk auf die in **Art. 4 Nr. 1 bis 26 DSGVO enthaltenen Begriffsbestimmungen** legen.
- Nicht alles muss neu gelernt werden: Wesentliche Prinzipien bleiben erhalten oder werden sogar noch gestärkt.
- Auch Aufsichtsbehörden sind dabei herauszufinden, wie sich „das Leben“ mit der DSGVO „anfühlt“!

- **DSGVO** entwickelt bekannte **Grundprinzipien** aus dt. Recht fort:

  Bsp. 1: Verbot mit Erlaubnisvorbehalt

  Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung

  *(1) Die Verarbeitung ist **nur rechtmäßig, wenn** mindestens eine der nachstehenden Bedingungen erfüllt ist: …*

  *c) die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt; …*

  *e) die Verarbeitung ist für die **Wahrnehmung einer Aufgabe** erforderlich, die im **öffentlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; …*

  (3) Die Rechtsgrundlage für die Verarbeitungen nach Absatz 1 Buchstaben c und e wird festgelegt durch

  a) Unionsrecht oder

  *b) das **Recht der Mitgliedstaaten**, dem der Verantwortliche unterliegt.*

→ Verarbeitung von Daten sonst i.d.R. nur mit **Einwilligung** zulässig!

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Szenario 2 - Mitarbeiterdaten

- BEKANNTMACHUNGEN
- WIR ÜBER UNS
- PERSONEN
- STANDORTE
- ZIELGRUPPEN
- DIENSTE
- RICHTLINIEN
- KONTAKT

Herzlich Willkommen beim IT-Service der Fakultät für Physik

Die Rechnerbetriebsgruppe ist zuständig für den IT-Service an der Fakultät für Physik. Sie bietet zentrale EDV-Dienste für alle Lehrstühle / Arbeitsgruppen und zentralen Einrichtungen sowie für alle Studierenden an. Die Administration der Rechner-Pools erfolgt dezentral an den verschiedenen räumlichen Standorten der Fakultät.

Hinweis für Erstsemester

Als Studenten der Fakultät verfügen Sie neben dem LMU-Postfach über ein weiteres Email Postfach bei der Fakultät. Am besten leiten Sie das LMU-Postfach auf Ihr Physik-Postfach

Bekanntmach

27.12.2016
Schutz vor Ma
Office Files mit

20.02.2015
Einstellung po
Das veraltete

02.02.2015
Email und aus
Was ist die bes

Daniela Aldea

Systemadministratorin

+49 (0) 89 / 2180 - 4519
daniela.aldea@physik.uni-muenchen.de
Raum: A021

Veronika Finsterwalder, Dipl. Inf. (FH)

Systemadministratorin, macOS
Systemintegration von macOS an der Fakultät

+49 (0) 89 / 2180 - 4521
veronika.finsterwalder@physik.uni-muenchen.de
Raum: A021

Ralph Heuer, Dipl. Inf. (FH)

Systemadministrator
Windows-Server Fakultät Physik
Windows-Kompetenzgruppe

+49 (0) 89 / 2180 - 4522
ralph.heuer@physik.uni-muenchen.de

Standortadministratoren

Susanna Maurer, Dipl.-Ing.

Standortadministratorin
CIP-Pool
Systemadministration
Netzwerkverwaltung
Benutzerverwaltung
Masteruser (LRZ)
Web-Administration

+49 (0) 89 / 2180 - 3976
maurer@physik.uni-muenchen.de
Raum: H508

Dr. Felix Rauscher

Standortadministrator Garching

+49 (0) 89 / 2891 - 4135
Felix.Rauscher@physik.uni-muenchen.de
Raum: 117

Ralph Simmler, Dipl.-Ing. (FH)

Standortadministrator
Theresienstraße
Linux
Windows
Serverraum
SGE
Beschaffung

+49 (0) 89 / 2180 - 4531
simmler@lmu.de
Raum: A020

Klaus Steinberger, Dipl.-Ing. (FH)

Standortadministrator
Zentrale Systeme (Garching)
Zentrale Systeme
Garching
Mailserveradministration

+49 (0) 89 / 289 - 14287
klaus.steinberger@physik.uni-muenchen.de
Raum: A021

Matthias Tischler

Standortadministrator
Geschäftsstelle
Windows-Server Fakultät Physik
Sprecher Windows-Kompetenzgruppe
Desktop- und Serversupport
Geschäftsstelle Physik
Ausbilder für Fachinformatiker / Systemintegration

+49 (0) 89 / 2180 - 5349
matthias.tischler@physik.uni-muenchen.de
Raum: 510

Bsp. 2: Grundsatz der Datensparsamkeit (Art. 5 Abs. 1 lit. c DSGVO) ?

„Personenbezogene Daten müssen… dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein ("Datenminimierung")“

Einwilligung, *Artikel 6 Nr.1a* DSGVO

- Auch in Zukunft wesentliche Rechtmäßigkeitsvoraussetzung für den Umgang mit personenbezogenen Daten ohne gesetzliche Grundlage
- Schriftform nicht (mehr) erforderlich.
- Verantwortlicher hat Nachweispflicht für Bestehen (Art. 7 DSGVO)
- Bisher erteilte Einwilligungen (nach Art. 15 BayDSG) gelten i.d.R. fort.
- Aber: Erweiterte Informationspflichten (Art.12 bis 14 DSGVO):
  → präzise, transparent, verständlich, in leicht zugänglicher Form (erst recht bei Verarbeitung sensibler Daten gem. Art. 9 DSGVO)
- Freiwillig (u.U. problem. im Arbeitsverhältnis)
- Kann jederzeit widerrufen werden, soweit sie nicht per Dienstvereinbarung abgegeben wird.
- **EMPFEHLUNG**: „alte“ Einwilligungen soweit wie möglich zeitnah aktualisieren und bei neuen Einwilligungen die Rechtsvoraussetzungen genau beachten!

Art. 13 DSGVO

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

- **Technischer Datenschutz - Datensicherheit**
  - Als **zentrales Prinzip** des Datenschutzes gesetzlich verankert (Art. 5 Abs. 1 lit. f und Art. 32 DSGVO).
  - WAS? Vertraulichkeit, Integrität und Verfügbarkeit und Belastbarkeit der Systeme gewährleisten
  - WOZU?: Angemessenes Sicherheitslevel im Verhältnis zum Risiko
  - WER? Verantwortliche und Auftragsverarbeiter
  - WIE?
    - Durch geeignete technische und organisatorische Maßnahmen
    - sowie die unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** sowie der Art, der Umstände und Zweck der Datenverarbeitung, der **unterschiedlichen Eintrittswahrscheinlichkeit** und **Schwere des Risikos** für die persönlichen Rechte und Freiheiten
    - Regelbeispiele: Pseudonymisierung; Verschlüsselung

- Begrenzung durch „**Stand der Technik**“ und „**Implementierungskosten**“?
- Identische Formulierung in Art. 32 „**Sicherheit d. Verarbeitung**“

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßn ausgelegt sind, die Datenschutzgrundsätze wie etwa Daten Garantien in die Verarbeitung aufzunehmen, um den Anforde betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und o Voreinstellung grundsätzlich nur personenbezogene Daten, d tungszweck erforderlich ist, verarbeitet werden. Diese Ver bezogenen Daten, den Umfang ihrer Verarbeitung, ihre Sp müssen insbesondere sicherstellen, dass personenbezogene Person einer unbestimmten Zahl von natürlichen Personen zu

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Art Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artik

Artikel 32

Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des U Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und S Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftrag geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schut gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

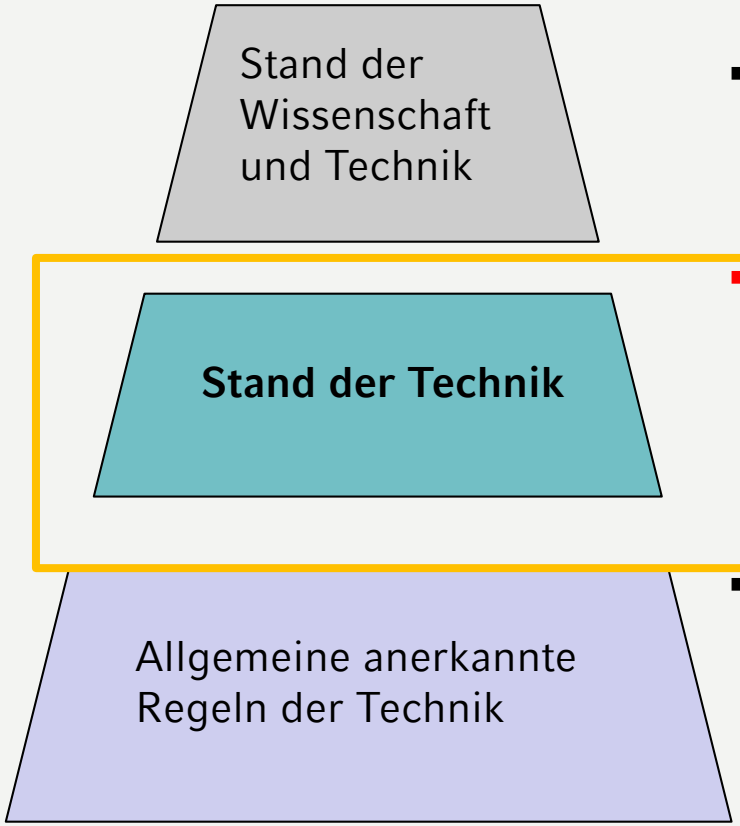
a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem phys technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der techr organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Geforderter Schutzstandard



- **Stand der Wissenschaft und Technik**
  = technische Spitzenleistungen, die wissenschaftlich gesichert sind (Laborversuch, wiss. Fachpublikation)
- **Stand der Technik**
  = fortschrittliche Verfahren, Einrichtungen oder Betriebsweisen, die in der Praxis geeignet erscheinen, die bestmögliche Begrenzung von Gefahren zu sichern, technisch erprobt u. am Markt verfügbar sind.
- **allgemein anerkannte Regeln der Technik**
  = technische Verfahren und Vorgehensweisen, die in der praktischen Anwendbarkeit erprobt sind und von der Mehrheit der Fachleute anerkannt werden. (z.B. DIN-Normen)

Art. 32

Anforderungen an die Sicherheit der Verarbeitung

(1) Art. 32 Abs. 3 und 4 DSGV findet keine Anwendung.

(2) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche oder der Auftragsverarbeiter auf Grundlage einer Risikobewertung Maßnahmen zu ergreifen, die geeignet sind, um

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle),
3. zu verhindern, dass
   a) Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
   b) personenbezogene Daten unbefugt eingegeben werden sowie gespeicherte personenbezogene Daten unbefugt gelesen, verändert oder gelöscht werden (Speicherkontrolle),
   c) automatisierte Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
   d) bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
4. zu gewährleisten, dass
   a) die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
   b) überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
   c) nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
   d) eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung),
   e) alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
   f) gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
   g) personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können (Auftragskontrolle).

Entwurf BayDSG, Stand: 28.09.2017

Wiederkehr von Art. 7 BayDSG?

Zielkonflikte

***Aufgaben des Verantwortlichen (nicht DSB!)**

- Führung des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung der Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Leitung*

- Störungsfreier Betrieb (QoS; SLAs)
- Kosten
- **Regelkonformität (Legalität)**

Ressourcen

- Personal
- Budget für
  - Schulung
  - Consulting
  - …

Risiken

- Wissensschaden (absoluter Datenverlust oder ungew. Bekanntgabe)
- Moral. Schaden
- Vermögensschaden
- Imageschaden
- Maßnahmen der Aufsichtsbehörde (Vor-Ort-Prüfungen, Anordnungen, Untersagungen)

Nutzer

- Bequemlichkeit
- Know-How

- **Was ändert sich beim „Verfahrensverzeichnis“?**
  - Jetzt: „**Verzeichnis von Verarbeitungstätigkeiten**“ → enthält **alle Verfahren**, nicht nur solche, für die eine Datenschutz-Folgenabschätzung durchgeführt wurde.
  - enthält eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** und eignet sich daher nicht für eine Veröffentlichung.
  - Recht auf kostenfreie Einsichtnahme für jeden ist nicht mehr vorgesehen.
  - vom „Verantwortlichen“ zu führen, also von der Behörde oder öffentlichen Stelle, die über die Verarbeitung entscheidet (Art. 4 Nr. 7 DSGVO), nicht mehr - wie das Verfahrensverzeichnis nach Art. 26 Abs. 1 BayDSG – rechtlich zwingend vom behördlichen DSB!
  - Erstellung und Betreuung kann allerdings von dem Behördenleiter dem behördlichen DSB übertragen werden.

Datenschutz-Folgenabschätzung (Art. 35 DSGVO)
(vormals „Vorabkontrolle“)

- Erforderlich für den Fall, dass eine konkret durchgeführte Verarbeitungstätigkeit ein **hohes Risiko für die Rechte und Freiheiten der Betroffenen** mit sich bringt.
- Erwägungsgrund 75: etwa anzunehmen bei Diskriminierung, **Identitätsdiebstahl**, finanziellem Verlust, Rufschädigung oder Profilbildung mit Standortdaten.
- Orientierung künftig an Liste der Aufsichtsbehörden
- Erfordert systematische Beschreibung der Verarbeitungsvorgänge und die Zwecke der Verarbeitung
- **Abwägung der Interessen** an der jeweiligen Verarbeitung (z.B. Einführung von Videoüberwachung) mit den Interessen der betroffenen Person an einem Unterlassen dieser Verarbeitung. Diese Abwägung ist zu dokumentieren.
- BayDSG-neu sowie Praxishilfen der Aufsichtsbehörden beachten!

Art. 14

Datenschutz-Folgenabschätzung

(zu Art. 35 DSGV)

(1) [1]Eine Datenschutz-Folgenabschätzung (Folgenabschätzung) durch den Verantwortlichen kann unterbleiben, soweit

1. eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Staatsministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird oder
2. der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine Folgenabschätzung erfolgt ist, es sei denn, dass in der Rechtsvorschrift etwas anderes bestimmt ist.

Entwurf BayDSG, Stand: 28.09.2017

---

[2]Die Staatsministerien können den öffentlichen Stellen die Ergebnisse der von ihnen und der von ihnen ermächtigten öffentlichen Stellen durchgeführten Folgenabschätzungen zur Verfügung stellen.

(2) [1]Entwickelt eine öffentliche Stelle ein automatisiertes Verfahren, das zum Einsatz durch öffentliche Stellen bestimmt ist, so kann sie, sofern die Voraussetzungen des Art. 35 Abs. 1 DSGV bei diesem Verfahren vorliegen, die Folgenabschätzung nach den Art. 35 und 36 DSGV durchführen. [2]Soweit das Verfahren von öffentlichen Stellen im Wesentlichen unverändert übernommen wird, kann eine weitere Folgenabschätzung durch die übernehmenden öffentlichen Stellen unterbleiben.

Szenario 3: Plagiatsprüfung

turnitin

OriginalityCheck®

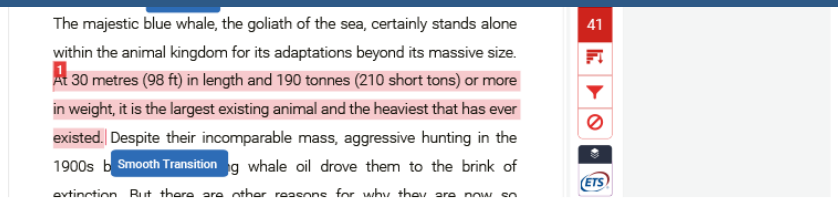
In der digitalen Welt von heute geschieht alles online – auch Plagiarismus. Aber Lehrkräfte können die Arbeiten Ihrer Studenten mit der genauesten Text-Datenbank der Welt abgleichen und mithilfe von Turnitin überprüfen, ob Studenten korrekt zitiert haben oder möglicherweise Plagiarismus vorliegt

Ephorus und Turnitin machen gemeinsame Sache !

Mehr Features

Bessere Technologie

Größere Datenbank



Zugang zur weltweit führenden Text-Datenbank

Die Datenbank von Turnitin enthält über 45 Milliarden aktuelle und archivierte Webseiten, über 337 Millionen Studentenarbeiten und über 130 Millionen von Artikeln aus Bibliotheken und Publikationen.

Code

Student no.

First name

Surname

E-mail

Comment

Document Durchsuchen... Keine Datei ausgewählt.

This text will be checked against other texts for similarities and will be saved in a database.

☐ agree

Send

- „Freiwilligkeit“?
- Datenschutzerklärung?
- Google Analytics?
- Auftrags(daten)verarbeitung / Speicherort?
- Verzeichnis der Verarbeitungstätigkeiten?
- Auskunftsersuchen?

Auftragsdatenverarbeitung

Betroffene Person

- Natürliche Person
- Besitzt Rechte („Datensubjekt“)

Verant-wortliche

- Entscheidet über Zweck und Art der Verarbeitung
- Verantwortlich gegenüber betroffenen Personen

Auftrags-verarbeiter

- Implementiert Anwendungen von Verantwortlichen

Auftragsdatenverarbeitung

- **Typische Fälle:**
  - Cloud-Computing
  - IT-Outsourcing (Bsp. LRZ)
  - Fernwartung durch IT-Dienstleister
  - Aktenvernichtung
- **NEU:**
  - Anhebung der techn./organis. Anforderungen auf den Stand der Technik
  - umfassende Mitwirkungspflichten (Melde-pflichten und DS-Folgeabschätzung).
  - Pflicht, eigenes Verzeichnis von Verarbeitungs-tätigkeiten zu führen.
- **Beachte:**
  - Bei zu ungenauer Beauftragung können Auf-tragsverarbeiter zu Verantwortlichen werden!
  - Mgl. Fokus der Aufsichtsbehörden auf ADV

Art. 28 DSGVO
Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

NEU: Mithaftung des Auftragsverarbeiters, Art. 82 DSGVO

"Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein … Schaden entstanden ist, hat Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter … Ein Auftragsverarbeiter haftet nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der … Anweisungen des … Verantwortlichen … gehandelt hat."

- **Beweislast** liegt bei Verantwortlichem bzw. Auftragsverarbeiter (vermutetes Verschulden), Art. 82 Abs. 3 EU-DSGVO
- **Gesamtschuldnerische Haftung** bei Schadensbeteiligung mehrerer, Art. 82 Abs. 4 EU-DSGVO
- Nicht verwechseln mit **Joint Controllership -** "Gemeinsam für die Verarbeitung Verantwortliche" des Art. 26 EU-DSGVO zu tun → dort AG UND AN verantwortliche Stelle.
- **Haftungsfreistellung** geben lassen? AGB-rechtlich zulässig?
- **Anpassung / „Nachverhandlung" bestehender Verträge?**

Rechte der Betroffenen

- Die **Informations- und Auskunftspflichten** werden deutlich umfangreicher.
- Es wird ein verbindliche **Reaktionszeit von einem Monat** eingeführt. Einmalig kann diese Frist um **zwei Monate** verlängert werden.
- Die betroffene Person ist hiervon innerhalb des ersten Monats unter Angabe der Gründe zu informieren.
- **Neu** sind
  - ***Recht auf „Vergessenwerden"*** *(Art. 17 DSGVO)* als Erweiterung des Rechts auf Löschen
  - ***Recht auf Datenübertragbarkeit („Portabilität"),*** *Art. 20 DSGVO*

Art. 20 DSGVO
Recht auf Datenübertragbarkeit

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und

b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

(3) Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4) Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Szenario 4 – verlorener Stick

Auszubildender V findet auf dem Mitarbeiter-Parkplatz des RZ einen USB-Stick. *Was wird er/sie damit anfangen?*

- *An der Pforte / im Fundbüro / im RZ abgeben.*
- *Am Dienstrechner einstecken und durchsuchen, um (u.a.) den Eigentümer oder Besitzer zu ermitteln.*
- *Am Dienstrechner einstecken, um die Speicherkapazität des Sticks zu ermitteln.*
- *Zu Hause einstecken, um nach interessanten Dokumenten, Bildern, Videos, Musik etc. suchen*

Dabei stellt er/sie fest, dass auf dem Stick u.a. der Mensaplan, der Entwurf des nächsten WAP-Antrags sowie Vorschläge für die Übernahme von Azubis nach Abschluss der Ausbildung gespeichert sind.

Muss der Vorfall gemeldet werden?
An wen?


17. Mai 2010, 21:01 Uhr Schwere Panne bei der Uni-Psychiatrie

Patientendaten auf dem Flohmarkt verkauft

"Es kommt beim Probanden zu Angstattacken": Was ein Rentner auf einer gebrauchten Festplatte fand.

Meldepflichten bei „Datenpannen“

- Art. 33 und 34 DSGVO: „Verletzungen des Schutzes personenbezogener Daten“ (also nicht nur sensibler Daten) sind
  - unverzüglich und möglichst **binnen 72 Stunden**
  - der **Aufsichtsbehörde** (= Landesbeauftr. f.d. Datenschutz) und ggf.
  - den **Betroffenen** gemeldet werden, **wenn** aus der Verletzung möglicherweise ein **hohes Risiko** für die persönlichen Rechte und Freiheiten entsteht.
- Ausnahme: Datenpanne führt „voraussichtlich“ nicht zu einem Risiko für den Betroffenen (= geeignete techn. und organisat. Maßnahmen getroffen, um zukünftige, gleichartige Datenschutzverstöße zu verhindern oder wirksame Maßnahmen zur Schadensbegrenzung ergriffen und diese das hohe Risiko eliminiert haben.
- Inhalt der Meldung bestimmt sich nach Art. 33 Abs. 3: Art der Datenpanne, Kategorien von betroffenen Daten, Anzahl der Betroffenen und der Datensätze
- **Schutzverletzungen sind** nach Art. 33 Abs. 5 **prüfbar zu dokumentieren**
- **Merkblatt mit Prozessbeschreibung für Mitarbeiter erstellen**

Maschinendaten

Szenario: „Einer klickt immer…“
Verw.angestellte E erhält eine gezielte Phishing-E-Mail, in der sie aufgefordert wird, ihr Passwort zurückzusetzen. E folgt den Anweisungen. Ihr Account wird im Anschluss missbraucht, um pers.bez. Daten zu übertragen.

Beispiel für Maschinendaten über den Zugriff auf eine Datei mit personenbezogenen Daten

- Enger Zeitrahmen für das Melden einer Sicherheitsverletzung verlangt robuste Prozesse für Erkennung, Untersuchung und int. Meldung von Sicherheitsverletzungen
- digitale Infrastruktur produziert riesige Mengen an Aktivitätsprotokollen, die zum Erkennen von Bedrohungen und Anomalien genutzt werden können
- „Logs“: = nützliche Aufzeichnungen zu den Aktivitäten im Zusammenhang mit Kunden, Benutzern, Transaktionen, Anwendungen, Servern, Netzwerken und Endgeräten
- liefern historischen Informationen um nachzuweisen, dass angemessene Sicherheitsvorkehrungen eingerichtet und proaktiv zur Risikominimierung eingesetzt wurden.

Datenschutz-Organisation

- Stellung des Datenschutzbeauftragten nach Art. 38 DSGVO ist mit der Stellung des behördlichen Datenschutzbeauftragten nach Art. 25 Abs. 2 bis 4 BayDSG vergleichbar.
- Künftig möglich: **Externer DSB**, Art. 38 Abs.5. Sinnvoll?

  Vor der Bestellung eines Externen DSB prüfen:
  - erforderliches Fachwissen in Fragen des auf die jeweilige Behörde oder öffentliche Stellen anzuwendenden Datenschutzrechts
  - Kenntnis der (behördl.) Datenschutzpraxis
  - gute Kenntnisse des Verwaltungsablaufs der öffentlichen Stelle

Art. 12

Behördliche Datenschutzbeauftragte

(zu Art. 35 Abs. 2, 37 bis 39 DSGV)

(1) [1]Behördliche Datenschutzbeauftragte erhalten insbesondere

1. Zugang zu dem Verzeichnis nach Art. 30 DSGV und
2. Gelegenheit zur Stellungnahme vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden.

[2]Art. 24 Abs. 5 bleibt unberührt.

(2) Behördliche Datenschutzbeauftragte dürfen Tatsachen, die ihnen in Ausübung ihrer Funktion anvertraut wurden, und die Identität der mitteilenden Personen nicht ohne deren Einverständnis offenbaren.

(3) Behördliche Datenschutzbeauftragte staatlicher Behörden können durch eine höhere Behörde bestellt werden.

Erweiterte Haftung für Verantwortliche

Risiken für Organisationen steigen im Hinblick auf zivilrechtliche Haftung wegen Datenschutzverstößen:

- Nach Art. 82 Abs. 1 DSGVO / Art. 37 BayDSG-E sind materielle und immaterielle Schäden zu erstatten, die auf Verstößen gegen die Verordnung beruhen.
- ausdrückliche Nennung immaterieller Schäden könnte zu einer erheblichen Veränderung gegenüber der bisherigen Rechtslage führen.
- Unterlassungsklagen denkbar

Art. 36 BayDSG-E

Vertrauliche Meldung von Datenschutzverstößen

[1]Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können. [2]Art. 12 Abs. 2 gilt für die zur Entgegennahme dieser Meldungen betraute Stelle entsprechend.

Wie sollte ich jetzt vorgehen (1/3)?

- Ermitteln Sie Ihren **Status-Quo**: Welche Ihrer gesammelten und gespeicherten Daten sind von den DSGVO betroffen?
  Entwickeln Sie einen Plan, um diese Daten aufzudecken.
- **Datenschutzdokumentation:** wichtiger denn je (Art. 5 Abs. 2 SGVO), bringen Sie daher alle datenschutz-relevanten Dokumente **auf den aktuellen Stand** (und versehen Sie diese bei der Gelegenheit mit Datum und Versionsnummer. Dies gilt insbesondere für
  - *Netzwerkübersicht, Soft- und Hardwareübersicht*
  - *(Internes) Verfahrensverzeichnis*
  - *Datenschutzkonzepte und -richtlinien:*
    z.B. Dokumentation der Zugangs- und Zugriffsberechtigungen sowie deren Pflege; gesicherte Anmelde- und Passwortverfahren; Nutzung von Verschlüsselungsverfahren; Portabilität, Löschung und Exportfähigkeit von Daten
  - *Dokument. angemessenen Schutzniveaus nach Stand der Technik*

Wie sollte ich jetzt vorgehen (2/3)?

- Überprüfen Sie auf Konformität
  - **Einwilligungserklärungen** (ggf. neu bei Betroffenen einholen)
  - Datenschutzrechtliche **Belehrungstexte** von Betroffenen (Datenschutzerklärung etc.) im Hinblick auf Artikel 13 und 14 DSGVO überarbeiten (= Sache der Leitung, nicht des DSB)
  - **Satzungen**
- Passen Sie die Verträge zur **Auftragsdatenverarbeitung** bzw. schließen Sie diese mit Dienstleistern neu ab
- Entwickeln bzw. überarbeiten Sie Ihr **Löschkonzept** und richten Sie ein Verfahren bei Anträgen auf Löschung ein
- Integrieren Sie **Privacy by Design / Default als Grundsätze** in den Entwicklungs-/ Betriebsprozess und berücksichtigen diese bei Ausschreibungen
- Etablieren Sie Verfahren, **Datenschutzverletzungen** zu erkennen.
- Implementieren Sie ein **Meldeverfahren bei Datenpannen**

Wie sollte ich jetzt vorgehen (3/3)?

- Schaffen Sie intern Systeme, die ermöglichen, dass Anfragen und Auskunftsersuchen von Betroffenen sehr kurzfristig und mit wenig Personalaufwand beantwortet werden können.
- Sicherstellen, dass bei allen Einführungen neuer und Änderungen bestehender Systeme der Datenschutz einbezogen wird.
- Datenschutzbeauftragten und Mitarbeitern Zeit und Möglichkeiten geben, um sich mit der EU-DSGVO zu beschäftigen.

Nehmen Sie den Datenschutz in der Hochschule ernst!

- Jeder (Fach)Verantwortliche ist als Mitarbeiter zugleich „Betroffener“
- Stellen Sie sowohl Technik als auch Prozesse auf den Prüfstand!
- Anordnungen und Verbote durch Aufsichtsbehörde wahrscheinlicher (Bsp.: Rechtmäßiger Einsatz von Videoüberwachung → erfordert heute „Datenschutz für Fortgeschrittene“)

LMU Rechtsinformatikzentrum

https://www.datenschutz-bayern.de/datenschutzreform2018/

https://www.lda.bayern.de/de/datenschutz_eu.html

Kontakt:

Ludwig-Maximilians-Universität
Rechtsinformatikzentrum
Prof.-Huber-Platz 2
80539 München
thomas.Hofer@lmu.de
Tel. 089/2180-2752