

# Datenschutz nach EU-Datenschutz-Grundverordnung Ihre Rechte, unsere Aufgaben

Guido Drexel

Datenschutzbeauftragter  
Bayerische Akademie der Wissenschaften  
datenschutzbeauftragter@badw.de  
datenschutz@badw.de

Bayerische Akademie der Wissenschaften – 22. Juni 2018

# Teil I: Grundlagen

- ▶ Datenschutz vs. Datensicherheit
- ▶ Grundsätze der Verarbeitung
- ▶ Begriffsbestimmungen  
personenbezogene Daten, Verarbeitung, verantwortliche Stelle,  
Pseudonymisierung, Dateisystem
- ▶ Informationspflichten
- ▶ Betroffenenrechte
- ▶ Sicherheit der Verarbeitung
- ▶ Meldepflichten
- ▶ Verzeichnis der Verarbeitungstätigkeiten
- ▶ Aufgaben und Stellung des Datenschutzbeauftragten

# Datenschutz vs. Datensicherheit

## Datenschutz

Schutz der Persönlichkeitsrechte.

Schutz von natürlichen Personen vor den nachteiligen Folgen einer Datenverarbeitung.

## Datensicherheit

Maßnahmen zum Schutz der Daten vor unbefugtem Zugriff, vor Mißbrauch etc.

Datensicherheit ist durch technische und organisatorische Vorgaben in der DSGVO festgeschrieben.

# Grundsatz

## Verbot mit Erlaubnisvorbehalt

Grundsätzlich ist verboten, was nicht ausdrücklich erlaubt ist!

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt. Erhebung, Verarbeitung und Nutzung von Daten sind verboten, es sei denn,

- ▶ sie sind durch eine Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder
- ▶ der Betroffene hat seine Einwilligung dazu erklärt.

### **Rechenschaftspflicht**

Die verantwortliche Stelle muß die Einhaltung der Vorschriften nachweisen können (Art 5 Abs 2, Art 24 Abs 1).

### **Wirksamkeitsprüfung**

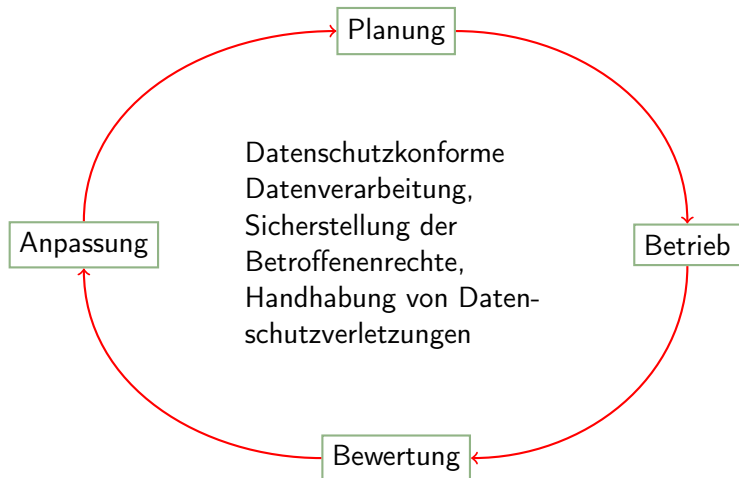
Die Wirksamkeit der technischen und organisatorischen Maßnahmen muß regelmäßig überprüft und bearbeitet werden (Art 24 Abs 1, Art 32 Abs 1 lit d).

### **Risikobasierter Ansatz**

Risiken für die Betroffenen feststellen und geeignete Maßnahmen festlegen.

# Datenschutzmanagement

Plan-Do-Check-Act, PDCA



# Begriffsbestimmungen

## Art 4 DSGVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

# Grundlagen

## Personenbezogene Daten

Personenbezogene Daten umfassen alle Angaben, mit denen Personen identifiziert werden können.

Name

Adresse

Alter

Geburtsdatum

Familienstand

Kfz-Kennzeichen

Gehalt

Augenfarbe

...

IP-Adresse

Telefonnummer

Bankkonto

Kreditkartennummer

eMail-Adresse

# Grundlagen

## Besondere Kategorien personenbezogener Daten

Besonders sensible Daten brauchen besonderen Schutz. Diese Daten heißen besondere Kategorien personenbezogener Daten (Art 9 DSGVO).

- ▶ rassistische und ethnische Herkunft
- ▶ politische Meinungen
- ▶ religiöse oder weltanschauliche Überzeugungen
- ▶ Gewerkschaftszugehörigkeit
- ▶ Angaben zur Gesundheit
- ▶ Angaben zum Sexualleben

# Begriffsbestimmungen

## Art 4 DSGVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

# Verarbeitungsphasen

erheben

speichern

verarbeiten

archivieren

übermitteln

löschen

Einhaltung der Rechenschaftspflicht schließt den Nachweis der datenschutz-konformen Verarbeitung über alle Phasen ein.

# Begriffsbestimmungen

## Art 4 DSGVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

7. „Verantwortlicher“ 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;

...

# Begriffsbestimmungen

## Art 4 DSGVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

# Begriffsbestimmungen

## Art 4 DSGVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

# Grundprinzipien I

nach Art 5 DSGVO

- ▶ **Rechtmäßigkeit und Transparenz**  
Welche Rechtsgrundlage gibt es für eine geplante Verarbeitung?
- ▶ **Zweckbindung**  
Sind die Zwecke der Verarbeitung festgelegt und dokumentiert?  
Ist sichergestellt, dass die Verarbeitung ausschließlich zu diesen Zwecken erfolgt?
- ▶ **Datensparsamkeit und Datenvermeidung**  
Werden nur Daten erhoben und verarbeitet, die für die festgelegten Zwecke angemessen und erforderlich sind?

# Grundprinzipien II

nach Art 5 DSGVO

- ▶ Richtigkeit  
Personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, müssen unverzüglich gelöscht oder berichtigt werden.
- ▶ Begrenzung der Datenspeicherung  
Personenbezogene Daten dürfen nicht länger gespeichert werden, als es für die Zwecke der Verarbeitung erforderlich ist.
- ▶ Integrität und Vertraulichkeit  
Personenbezogene Daten müssen so verarbeitet werden, dass eine angemessene Sicherheit gewährleistet ist.

# Bedingungen für die Einwilligung

nach Art 7 DSGVO

Soll eine Einwilligung Grundlage für eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten sein, so ist zu beachten:

- ▶ Der Verantwortliche muß nachweisen können, dass die betroffene Person in die Verarbeitung eingewilligt hat.
- ▶ Die Einwilligung hat in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen.
- ▶ Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Sie ist über dieses Widerrufsrecht vor der Einwilligung in Kenntnis zu setzen.
- ▶ Die Einwilligung hat freiwillig zu erfolgen. Es besteht ein Koppelungsverbot.

Die Informationspflichten nach Art 13 DSGVO sind zu beachten.

# Rechte der betroffenen Person

## Art 15 bis 22 DSGVO

- ▶ Auskunftsrecht der betroffenen Person  
Verarbeitung personenbezogener Daten? Zweck? Rechtsgrundlage? Speicherdauer? Übermittlung? Hinweis auf Rechte.
  - ▶ Recht auf Berichtigung
  - ▶ Recht auf Löschung d. h. „Recht auf Vergessenwerden“  
Zweck der Verarbeitung ist erloschen, Widerruf einer Einwilligung, unrechtmäßige Verarbeitung . . .
  - ▶ Recht auf Einschränkung der Verarbeitung
  - ▶ Mitteilungspflicht nach Berichtigung, Löschung, Einschränkung
  - ▶ Recht auf Datenübertragbarkeit
  - ▶ Widerspruchsrecht
  - ▶ Automatisierte Entscheidungen im Einzelfall, Profiling
- Bitte stets den Datenschutzbeauftragten informieren.

# Transparenz durch Information – Informationspflichten I

nach Art 13 DSGVO

Zum Zeitpunkt der Erhebung personenbezogener Daten sind der betroffenen Person die folgenden Informationen mitzuteilen.

- ▶ Namen und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
- ▶ Kontaktdaten des Datenschutzbeauftragten
- ▶ die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung
- ▶ sofern die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
- ▶ gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- ▶ gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln ...

# Transparenz durch Information – Informationspflichten II

nach Art 13 DSGVO

- ▶ Angaben zur Speicherdauer oder Kriterien für die Festlegung dieser Dauer
- ▶ Hinweis auf das Bestehen eines Rechts auf Auskunft über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung
- ▶ Hinweis auf das Bestehen eines Rechts auf Widerspruch gegen die Verarbeitung
- ▶ Hinweis auf das Bestehen eines Rechts auf Datenübertragbarkeit
- ▶ Hinweis auf das Bestehen eines Rechts auf Widerspruch gegen eine Einwilligung
- ▶ Hinweis auf das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde

# Transparenz durch Information – Informationspflichten III

nach Art 13 DSGVO

- ▶ Informationen, 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
- ▶ Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
- ▶ falls eine Zweckänderung geplant ist, so ist die betroffene Person vor der Weiterverarbeitung entsprechend zu informieren.

# Sicherheit der Verarbeitung

nach Art 32 DSGVO

- ▶ technische und organisatorische Maßnahmen unter Berücksichtigung von
  - ▶ Stand der Technik
  - ▶ Implementierungskosten und Umsetzungsaufwand
  - ▶ Art, Umfang, Umstände und Zwecke der Verarbeitung
  - ▶ Eintrittswahrscheinlichkeit und Schwere des Risikos
- ▶ zur Sicherstellung von
  - ▶ Vertraulichkeit
  - ▶ Integrität (unerwünschte Modifikation)
  - ▶ Verfügbarkeit
  - ▶ Belastbarkeit der Systeme
- ▶ Pseudonymisierung und Verschlüsselung personenbezogener Daten

# Datenschutz-Folgenabschätzung

nach Art 35 DSGVO

Feststellung, ob eine (geplante) Verarbeitungstätigkeit voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat.

—→ Maßnahmen zur Reduzierung potentieller Risiken

# Handhabung von Datenschutzverletzungen I

nach Art 33 DSGVO

Der Verantwortliche meldet unverzüglich und möglichst binnen 72 Stunden an die zuständige Aufsichtsbehörde, außer dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Meldung enthält zumindest die folgenden Informationen:

- ▶ Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
- ▶ Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- ▶ Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen

# Handhabung von Datenschutzverletzungen II

nach Art 33 DSGVO

- ▶ Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
  - ▶ Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- Bitte stets den Datenschutzbeauftragten informieren.

# Verzeichnis der Verarbeitungstätigkeiten

nach Art 30 DSGVO

- ▶ Namen und Kontaktdaten des Verantwortlichen
- ▶ Namen und Kontaktdaten des Datenschutzbeauftragten
- ▶ Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- ▶ Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
- ▶ Empfänger (auch in Drittländern), gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden
- ▶ Sind Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation geplant?
- ▶ Fristen für die Löschung der verschiedenen Datenkategorien
- ▶ Beschreibung der technischen und organisatorischen Maßnahmen

# Verzeichnis der Verarbeitungstätigkeiten

ergänzende Angaben zur Erfüllung der Informationspflichten

- ▶ allgemeine Beschreibung der Verarbeitungstätigkeit
- ▶ Rechtsgrundlage für die Verarbeitung
- ▶ Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
- ▶ Sicherheitskonzept zum Nachweis der technischen und organisatorischen Maßnahmen
- ▶ Klassifikation der Risiken für die Rechte und Freiheiten betroffener Personen

# Verzeichnis der Verarbeitungstätigkeiten

## am Beispiel *Bayerisches Wörterbuch*

### Projekt „Bayerisches Wörterbuch“

#### Verarbeitungsverzeichnis nach DS-GVO

Stand: 11.06.2018/UW

<b>Verantwortlicher</b> Bayerische Akademie der Wissenschaften Projekt „Bayerisches Wörterbuch“ Alfons-Goppel-Straße 11, 80539 München Tel. +49 (0)89 23031-0, E-Mail: info@badw.de Projektleiter: Professor Dr. Anthony Rowley	<b>Datenschutzbeauftragter</b> Guido Drexel Leibniz-Rechenzentrum, Boltzmannstraße 1, 85748 Garching bei München Zimmer I.1.027, Telefon +49 (0)89 35831 – 8738, <a href="mailto:datschutz@badw.de">datschutz@badw.de</a>
--	--

#### Gewährpersonen für die Fragebogen (= Lieferanten der Mundartbegriffe fürs Wörterbuch)

Die DSGVO gilt nur für lebende Personen (Erwägungsgrund 27). Die älteren Befragungsrunden (1913-1934) sind daher wohl nicht mehr betroffen. Die Wörterlisten werden seit 1958 versandt.

RECHTSGRUNDLAGE: „freiwillige Einwilligung“ nach Art. 6 (1) a DS-GVO

Gemeinsam Verantwortliche	Zweck	Betroffenen- gruppen	Datenkategorien	Empfänger	Übermittlung von pD	Löschfrist	Technisch-organisatorische Maßnahmen
BWB	a) Adressverwaltung: Kommunikation mit den GP	Alle Sammler (= Gewährspersonen)	Kontaktdaten, Sammlungsgebiet, Beruf, Jahrgang, Erhebungen; ggf. Medaillen, Grund des Ausscheidens	Redaktion	Keine	Keine	liegt vor als Exeldatei und als Outlookverteiler; Datei liegt im Zugriffsgeschützten Server-Verzeichnis
BWB	b) Publikation in Printform (Beiheft): Nachweis der Sammler (GP) für die Mundartbegriffe im Sinn von Belegbarkeit der wiss. Forschungsergebnisse + öffentlicher Dank an die ehrenamtlichen GP	Alle Sammler (= Gewährspersonen)	Sammlungsgebiet, Beruf, Erhebungen	Print-Publikation	Keine	Keine	Einverständnis der GP für Veröffentlichung vorhanden (siehe Erläuterung in Datei BWB-pD_2018-05-15.docx)
BWB	c) Publikation auf Website: <a href="http://bwb.badw.de/materialsammlung/sammlerverzeichnis.html">http://bwb.badw.de/materialsammlung/sammlerverzeichnis.html</a> Zweck wie b)	Alle Sammler (= Gewährspersonen)	Sammlungsgebiet, Beruf, Erhebungen	Nutzer der Website	Web	Keine	Siehe b)

# Stellung des Datenschutzbeauftragten

nach Art 38 DSGVO

- ▶ frühzeitige Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen
- ▶ Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen
- ▶ Zur-Verfügung-Stellung der erforderlichen Ressourcen
- ▶ Weisungsfreiheit
- ▶ Beratung betroffener Personen
- ▶ ...

# Aufgaben des Datenschutzbeauftragten

nach Art 39 DSGVO

- ▶ Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen
- ▶ Überwachung der Einhaltung der Datenschutzvorschriften
- ▶ Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
- ▶ Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung
- ▶ Zusammenarbeit mit der Aufsichtsbehörde
- ▶ ...

### Artikel 6 – Zweckbindung

- (3) Eine Verarbeitung zu anderen Zwecken als zu denjenigen, zu denen die Daten erhoben wurden, ist unbeschadet der Bestimmungen der DSGVO zulässig, wenn

...

3. die Verarbeitung erforderlich ist

...

- c) zur Durchführung wissenschaftlicher oder historischer Forschung, das wissenschaftliche oder historische Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann

# Bayerisches Datenschutzgesetz

## Art 25 Abs 1-2 BayDSG

### Artikel 25 – Verarbeitung zu Forschungszwecken (zu Art. 89 DSGVO)

- (1) Für Zwecke der wissenschaftlichen oder historischen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet werden.
- (2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können, gesondert zu speichern. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

# Bayerisches Datenschutzgesetz

## Art 25 Abs 3-4 BayDSG

Forts. Artikel 25 – Verarbeitung zu Forschungszwecken

- (3) Die wissenschaftliche oder historische Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.
- (4) Die Art. 15, 16, 18 und 21 DSGVO sind nicht anzuwenden, soweit die Inanspruchnahme dieser Rechte voraussichtlich die Verwirklichung der wissenschaftlichen oder historischen Forschungszwecke unmöglich macht oder ernsthaft beeinträchtigt und diese Beschränkung für die Erfüllung der Forschungszwecke notwendig ist.

## II. Einzelthemen

- ▶ Telearbeit
- ▶ Datenschutzerklärung
- ▶ Foto und Film
- ▶ Newsletter
- ▶ Bewerbungen
- ▶ unbeabsichtigte Offenlegung
- ▶ *Social Media*
- ▶ Dropbox, Skype, WhatsApp & Co.

# Telearbeit. Das verlangen die Aufsichtsbehörden

nach DatenschutzPraxis, 05/2018, Seite 13

1. Der DSB ist beteiligt.
2. Die datenschutzrechtliche Verantwortung ist individuell vertraglich festgelegt.
3. Arbeitgeber, DSB und Datenschutzaufsichtsbehörde haben Zutrittsberechtigung zum Arbeitsplatz.
4. Arbeitsplatz und Arbeitgebernetzwerk sind per Virtual Private Network (VPN) verbunden.
5. Es erfolgt kein Transport von Dokumenten zwischen Büro- und Tele-Arbeitsplatz.
6. Es ist ausgeschlossen, dass Mitbewohner und Besucher die Daten zur Kenntnis nehmen, nutzen oder manipulieren können.
7. ...

# Transparenz durch Information – Datenschutzerklärung I

nach Art 13 DSGVO

siehe Datenschutzerklärung

<http://badw.de/data/footer-navigation/datenschutz.html>

und <https://www.lrz.de/datenschutzerklaerung/>

- ▶ Namen und Kontaktdaten des Verantwortlichen
- ▶ Kontaktdaten des Datenschutzbeauftragten
- ▶ Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
- ▶ Rechtsgrundlage für die Verarbeitung
- ▶ Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- ▶ Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln . . .

# Transparenz durch Information – Datenschutzerklärung II

nach Art 13 DSGVO

- ▶ Angaben zur Speicherdauer oder Kriterien für die Festlegung dieser Dauer
- ▶ Hinweis auf die Rechte der betroffenen Person d. h. Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruchsrechte nach Art 21 DSGVO
- ▶ Die Datenschutzerklärung muß darüber aufklären, ob der Nutzer für bestimmte Zwecke Daten bereitstellen muß und welche Konsequenzen es hat, wenn er dies verweigert.
- ▶ Beschwerderecht bei der Aufsichtsbehörde mit Angabe der für die Einrichtung zuständigen Aufsichtsbehörde
- ▶ (Nicht-)Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling

# Bewerbungen

- ▶ stets die zuständige Personalabteilung einbeziehen
- ▶ Informationspflichten beachten
- ▶ Einwilligung des Bewerbers zur Verarbeitung, Speicherung etc. einholen
- ▶ Löschfristen beachten

# Foto- und Filmaufnahmen

Ein Foto gilt als personenbezogenes Datum, wenn eine Person identifizierbar ist. Ergo ist die DSGVO anwendbares Recht.

Maßgebliche Rechtsgrundlage ist daher nach Art 6 DSGVO zu bestimmen, Informationspflichten nach Art 13 sind zu beachten i. e. Zweck, Kontaktdaten etc.

Das Kunsturhebergesetz (KUG) regelt in § 22 Satz 1 lediglich die Verbreitung: *Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.*

Unter welchen Voraussetzungen Abbildungen von Personen angefertigt werden dürfen, regelt KUG nicht.

# Newsletter I

nach LfDI BW, 33. Tätigkeitsbericht 2016/2017, Seite 119

- ▶ Verschlüsselung: Wird die Newsletter-Anmelde-Internetseite per https übertragen?
- ▶ Wird klar und eindeutig beschrieben, wer verantwortliche Stelle ist und um welchen Inhalt/welche Inhalte es bei dem Newsletter geht?
- ▶ Wird bei der Anmeldung darauf hingewiesen, dass der Betroffene dem Newsletter-Bezug jederzeit widersprechen kann?
- ▶ Welche Daten werden als Pflichtfelder abgefragt (z.B. eMail-Adresse, PLZ, Wohnort, Straße und Hausnummer, Vor- und Nachname usw.)?
- ▶ Wird die Anmeldung durch ein Double-Opt-in-Verfahren vollzogen?
- ▶ Wenn ja: Ist die Bestätigungs-eMail frei von jeglicher Werbung?

# Newsletter II

nach LfDI BW, 33. Tätigkeitsbericht 2016/2017, Seite 119

- ▶ Welche weiteren Daten werden bei der Anmeldung gespeichert (z.B. IP-Adresse, Datum/Uhrzeit)?
- ▶ Wird der Newsletter in der Datenschutzerklärung vollständig beschrieben?
- ▶ Wird in jedem Newsletter darauf hingewiesen, dass der Betroffene dem Newsletter-Bezug jederzeit widersprechen kann?
- ▶ Ist die Abbestellung dann ohne besonderen Aufwand mit einem Klick möglich?
- ▶ Liegen Einwilligungen aller Bezieher des Newsletters vor?
- ▶ Werden Adressaten eines nicht zustellbarer Newsletters gelöscht?

# Datenschutzverletzungen

- ▶ Ausdruck mit personenbezogenen Daten wie Bewerbungsunterlagen zu lange an einem Drucker liegen gelassen
- ▶ einen offenen eMail-Verteiler verwendet, der neben den (bekannten) Instituts-eigenen Adressen viele externe aufführt
- ▶ einen USB-Speicher mit personenbezogenen Daten verloren
- ▶ ...

# EuGH zur Mitverantwortlichkeit bei Facebook-Fanpages I

EuGH C-210/16, Aufzählung folgt DSK-Entschließung

- ▶ Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.
- ▶ Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.
- ▶ Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der DS-GVO erfüllt.

# EuGH zur Mitverantwortlichkeit bei Facebook-Fanpages II

EuGH C-210/16, Aufzählung folgt DSK-EntschlieÙung

- ▶ Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DSGVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

## dienstliche Nutzung von ...

Dropbox → <https://syncandshare.lrz.de/>

Skype → <https://meet.lrz.de/>

WhatsApp → - ? -

<https://www.google.de/> → <https://www.startpage.com/>

Startpage

<https://www.startpage.com/>

“Privacy is a  
basic human right.”

Robert E.G. Beens

STARTPAGE CEO

# Aufsichtsbehörden

Europa – Deutschland – Bayern

EDSB – Der Europäische Datenschutzbeauftragte

<https://edps.europa.eu/>

BfDI – Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

<https://www.datenschutz.bund.de/>

<https://www.datenschutzforum.bund.de/>

BayLfD – Der Bayerische Landesbeauftragte für den Datenschutz

<https://www.datenschutz-bayern.de/>

BayLDA – Bayerisches Landesamt für die Datenschutzaufsicht

<https://www.lda.bayern.de/>

Vielen Dank für Ihre Aufmerksamkeit.

Fragen – Kommentare – Anregungen?

`datenschutz@badw.de`  
`datenschutz@wmi.badw.de`  
`datenschutz@lrz.de`