Rechtsinformatikzentrum
Thomas Hofer, Akad. Direktor

Die EU-Datenschutz-Grundverordnung aus Behördensicht

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 BVS
- IT-Security-Beauftragter (TÜV PersCert) und Compliance-Manager

Meine Ziele:

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

Agenda

Was Behördenleitung und Fachverantwortliche wissen müssen, um Ihre Einrichtung fit für das neue Datenschutzrecht zu machen…

- *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?*

Ausgangslage

Art. 1 Bayerisches Datenschutzgesetz:

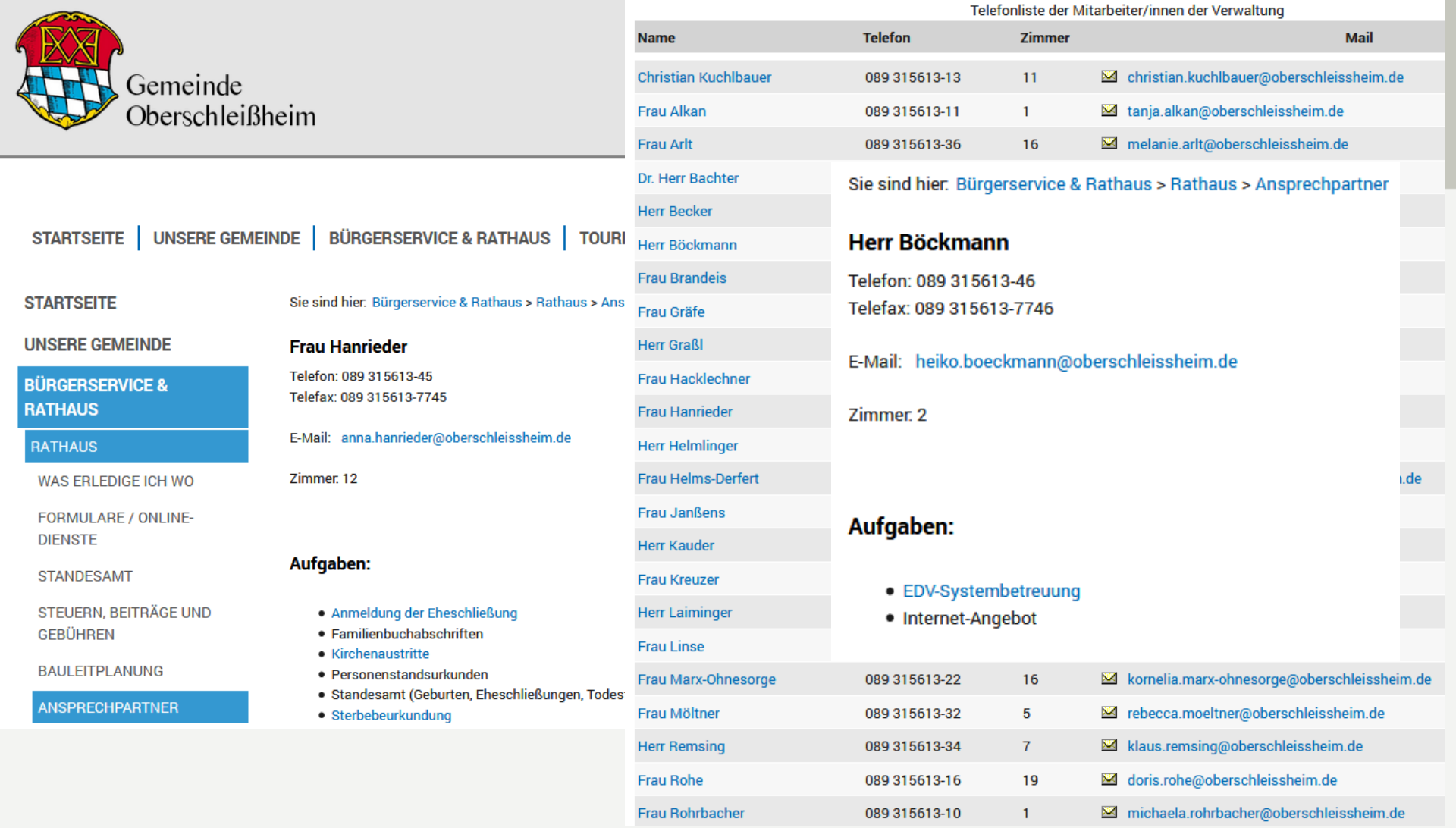
„Zweck dieses Gesetzes ist es, die Einzelnen davor zu schützen, dass sie bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch öffentliche Stellen in unzulässiger Weise in ihrem Persönlichkeitsrecht beeinträchtigt werden.“

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. Diese werden gefordert durch:
  - das allgemeine Persönlichkeitsrecht (Art. 1 und Art. 2 GG, *Artikel 8 Abs. 1 der Charta der Grundrechte der Europäischen Union, Artikel 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)*)
  - das **Recht auf informationelle Selbstbestimmung (BVerfG)**



Gemeinde Oberschleißheim

STARTSEITE | UNSERE GEMEINDE | BÜRGERSERVICE & RATHAUS | TOURI

STARTSEITE

UNSERE GEMEINDE

BÜRGERSERVICE & RATHAUS

RATHAUS

WAS ERLEDIGE ICH WO

FORMULARE / ONLINE-DIENSTE

STANDESAMT

STEUERN, BEITRÄGE UND GEBÜHREN

BAULEITPLANUNG

ANSPRECHPARTNER

Sie sind hier: Bürgerservice & Rathaus > Rathaus > Ans

Frau Hanrieder

Telefon: 089 315613-45
Telefax: 089 315613-7745

E-Mail: anna.hanrieder@oberschleissheim.de

Zimmer: 12

Aufgaben:

- Anmeldung der Eheschließung
- Familienbuchabschriften
- Kirchenaustritte
- Personenstandsurkunden
- Standesamt (Geburten, Eheschließungen, Todes
- Sterbebeurkundung

Telefonliste der Mitarbeiter/innen der Verwaltung

Name	Telefon	Zimmer	Mail
Christian Kuchlbauer	089 315613-13	11	christian.kuchlbauer@oberschleissheim.de
Frau Alkan	089 315613-11	1	tanja.alkan@oberschleissheim.de
Frau Arlt	089 315613-36	16	melanie.arlt@oberschleissheim.de
Dr. Herr Bachter			
Herr Becker			
Herr Böckmann			
Frau Brandeis			
Frau Gräfe			
Herr Graßl			
Frau Hacklechner			
Frau Hanrieder			
Herr Helmlinger			
Frau Helms-Derfert			
Frau Janßens			
Herr Kauder			
Frau Kreuzer			
Herr Laiminger			
Frau Linse			
Frau Marx-Ohnesorge	089 315613-22	16	kornelia.marx-ohnesorge@oberschleissheim.de
Frau Möltner	089 315613-32	5	rebecca.moeltner@oberschleissheim.de
Herr Remsing	089 315613-34	7	klaus.remsing@oberschleissheim.de
Frau Rohe	089 315613-16	19	doris.rohe@oberschleissheim.de
Frau Rohrbacher	089 315613-10	1	michaela.rohrbacher@oberschleissheim.de

Sie sind hier: Bürgerservice & Rathaus > Rathaus > Ansprechpartner

Herr Böckmann

Telefon: 089 315613-46
Telefax: 089 315613-7746

E-Mail: heiko.boeckmann@oberschleissheim.de

Zimmer: 2

Aufgaben:

- EDV-Systembetreuung
- Internet-Angebot

- Geschützt wird die Freiheit, selbst über Verwendung und Preisgabe zu entscheiden (wer weiß was wann und bei welcher Gelegenheit über mich?)
- unabhängig davon, welcher Personengruppe der Betroffene angehört

Ausgangslage

Informationssicherheit

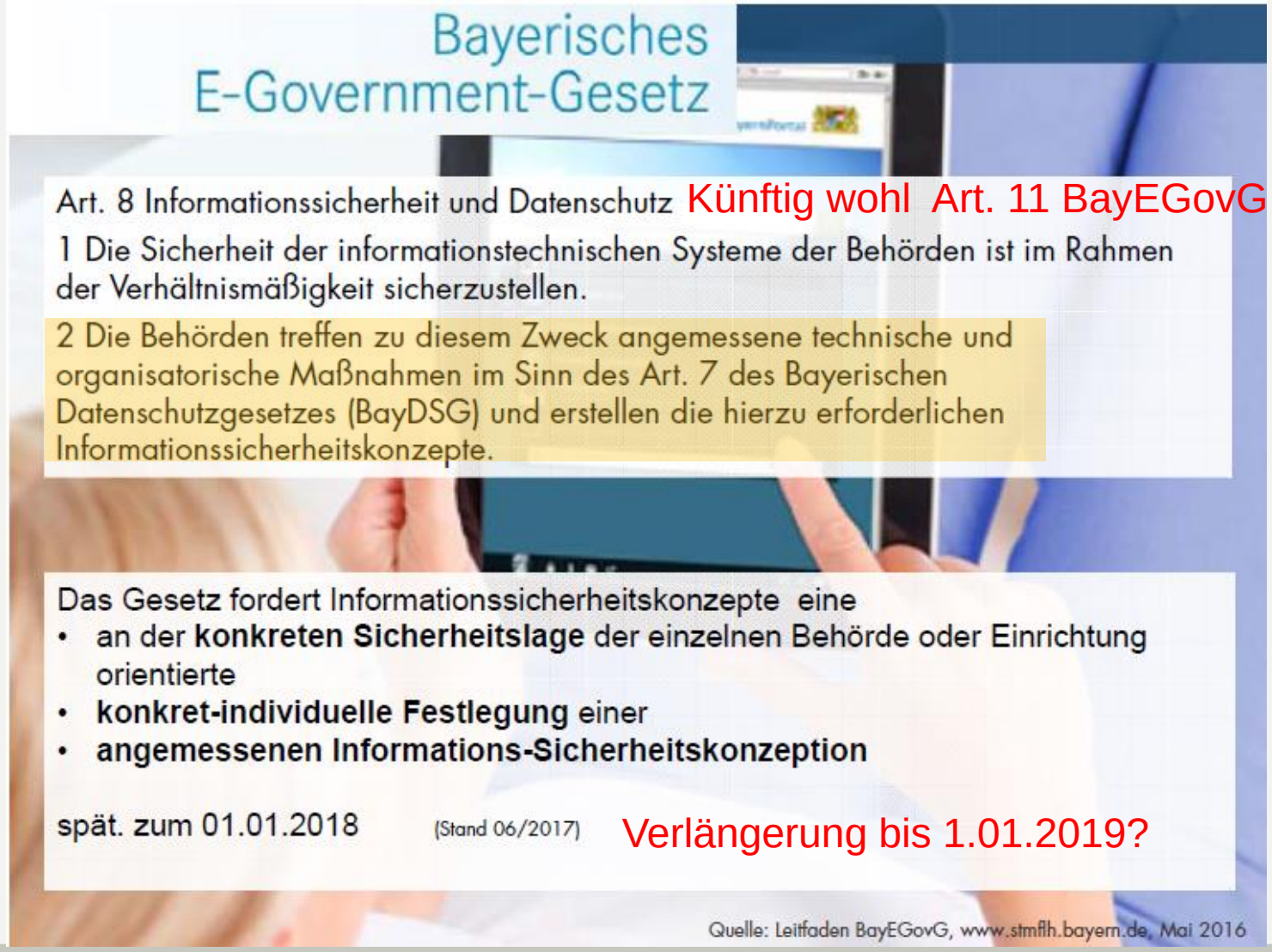
Schutzgut: alle relevanten Arten von Informationen jeglicher Art und Herkunft; Hard- und Software
Risiko: Verlust, Zerstörung, Vertraulichkeit, Missbrauch

TOM / TOV

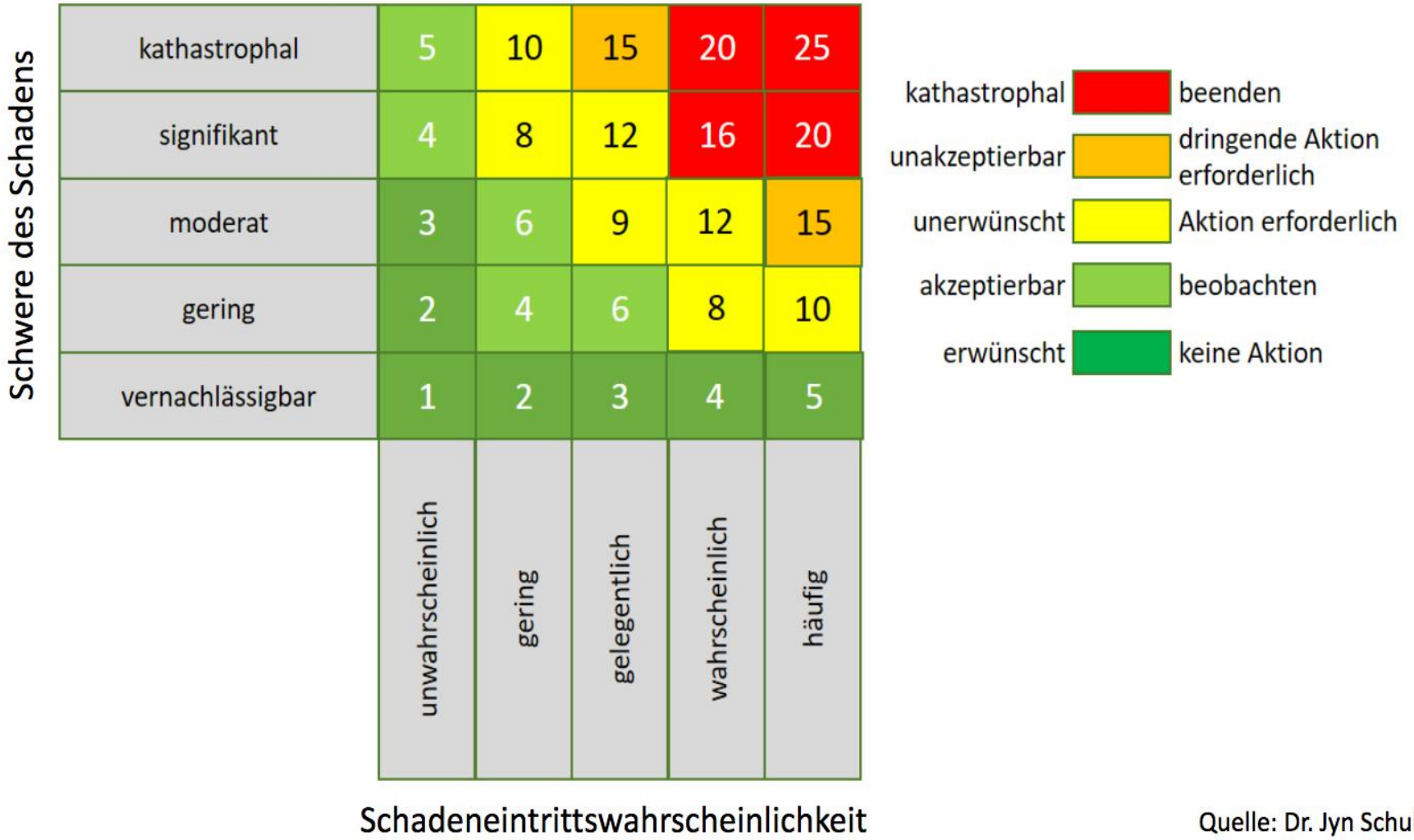
Datenschutz

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

Ausgangslage



Ausgangslage



Quelle: Dr. Jyn Schultze-Melling

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

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**.“

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

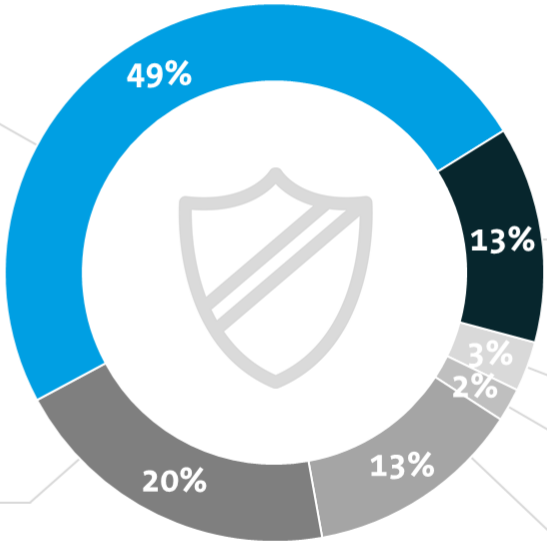
EU-Datenschutzgrundverordnung (DS-GVO)

- 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): 218 Tage (= ca. 31 Wochen)**
  - Abzüglich: Wochenende, Feier-, Krankheits-, Geburtstage, Fortbildungen, ...
  - Also: **nicht mehr ganz so viel Zeit!**

Jedes dritte Unternehmen ignoriert bislang die DS-GVO

Wie weit ist Ihr Unternehmen bei der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) zum aktuellen Zeitpunkt?

Und Sie??



Beschäftigen uns aktuell damit

Erste Maßnahmen angefangen und umgesetzt

Weiß nicht/k.A.

Ist uns überhaupt nicht bekannt

Werden uns damit bewusst nicht beschäftigen

Haben uns bislang noch nicht damit beschäftigt

Basis: Unternehmen ab 20 Mitarbeitern (n=507) | Quelle: Bitkom Research

bitkom

Wenn etwas neu ist,

…ist es für alle neu?!

…Institutionen, Begriffe, Definitionen, Auslegungen

(gilt selbst für bereits im BDSG / BayDSG verwendete Begriffe)

- Unerlässlich, sich mit (teilweise vom bisherigen Sprachgebrauch abweichenden) Begrifflichkeiten der DSGVO vertraut machen.
- Besonderes Augenmerk auf die in **Art. 4 Nr. 1 bis 26 DSGVO enthaltenen Begriffsbestimmungen** legen.
- Kleiner Trost: Nicht alles muss neu gelernt werden! Wesentliche Prinzipien des dt. DS-Rechts bleiben erhalten oder werden sogar noch gestärkt.
  - *Verbot mit Erlaubnisvorbehalt*
  - *Zweckbindung*
  - *Erforderlichkeit; Datensparsamkeit; Datenlöschung…*
- Auch Aufsichtsbehörden sind dabei herauszufinden, wie sich „das Leben“ mit der DSGVO „anfühlt“!
- Aber: Staatliche und kommunale öffentliche Stellen selbst für die Umsetzung der DSGVO verantwortlich.

- Zu berücksichtigende **Anforderungen der DSGVO** (Auszug):
  - **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
- **Neue Institute / Rechte** (Auszug):
  - **Art. 17: Recht auf Löschung („Vergessenwerden“)**
  - Art. 18: Recht auf Datenübertragbarkeit („Datenmitnahme“)
  - **Art. 25: Datenschutz durch Technik („Privacy by design“)**

Beispiel: Einwilligung, *Artikel 6 Nr.1a* DSGVO

- Auch in Zukunft eine wesentliche Rechtmäßigkeitsvoraussetzung für den Umgang mit personenbezogenen Daten ohne gesetzliche Grundlage
- Schriftform nicht (mehr) erforderlich. Bisher erteilte Einwilligungen nach Art. 15 BayDSG gelten in aller Regel fort.
- Aber **erweiterte Informationspflichten** (Art.12 bis 14 DSGVO): präziser, transparenter, verständlicher und leicht zugänglicher Form
- **EMPFEHLUNG**: „alte“ Einwilligungen soweit wie möglich zeitnah aktualisieren und bei neuen Einwilligungen die Rechtsvoraussetzungen genau beachten!

EU-Datenschutzgrundverordnung (DS-GVO)

- enthält einige sogenannte **Öffnungsklauseln**
  = Regelungsspielräume für Konkretisierungen, Ergänzungen oder Abweichungen von den Bestimmungen der DSGVO im nationalen Datenschutzrecht
  - in einigen Bereichen müssen die Nationalstaaten diese Öffnungsklauseln mit eigenen Regelungen ausfüllen.
  - In anderen Bereichen können sie die Öffnungsklauseln nutzen, um erprobte Datenschutzregelungen im nationalen Recht zu erhalten.
- Umsetzung der Öffnungsklauseln durch **Neufassung des BayDSG** sowie durch Änderungen im Fachrecht (Bsp.: Art. 24 der Gemeindeordnung erhält nun eine gesetzliche Rechtsgrundlage für den Einsatz elektronischer Wasserzähler)
- Ziel wie bisher: 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

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

Derzeit in Anhörung bei Verbänden

Materielle Neuerungen im Entwurf „BayDSG neu“:

- **Verarbeitung personenbezogener Daten zu journalistischen, künstlerischen und literarischen Zwecken** (Art. 38): Sie gilt nur, soweit das Presserecht, das Rundfunkrecht und das Medienrecht keine vorrangigen Sondervorschriften enthalten.
- **Verarbeitung personenbezogener Daten für die Verleihung staatlicher und kommunaler Auszeichnungen und Ehrungen** (Art. 27) **:** nun rechtlich abgesichert durch die Aufnahme einer eigenständigen Regelung. Diese ist notwendig, da für diesen Zweck auch besondere Kategorien personenbezogener Daten verarbeitet werden.

Was ist (wirklich) neu in der DSGVO?

- **Dokumentations- / Nachweispflichten** („accountability“):
  - Der Verantwortliche muss jederzeit auf Anfrage nachweisen können, dass er die Datenschutzgrundsätze einhält!
  - Organisationen müssen umfassender als bislang darüber informieren, ob und wie sie pb Daten verarbeiten
- **Risikobasierter Ansatz nach Stand der Technik: Grundrechtsbeeinträchtigung vs. Eintrittswahrscheinlichkeit**
- **Datenschutz durch Technikgestaltung**
- **Informationspflichten**
- **Erweitere Betroffenenrechte** (z.B. Reaktionsfrist auf Anfragen)
- **Verschärfte Meldepflicht** bei Schutzverletzungen
- **…**

Das neue Daten

- **Etwas mehr im Detail:**
  - Datenschutz durch Technik und datenschutzrechtliche Voreinstellungen (Privacy by Design, privacy by default): Prinzipien der Erforderlichkeit und Datenminimierung werden verbindlich. →Berücksichtigung in öffentlichen Ausschreibungen?
  - Externe behördliche Datenschutzbeauftragte (Art.37 Abs.6 DS-GVO)
- Aber: Weiterhin **keine 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.

- **Was ändert sich beim Verfahrensverzeichnis?**
  - Verzeichnis von Verarbeitungstätigkeiten enthält **alle Verfahren**, nicht nur solche, für die eine Datenschutz-Folgenabschätzung durchgeführt wurde.
  - Es 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.

Das neue Datens

- **Aufgaben des Verantwortlichen** (d.h. Behördenleitung) – und damit künftig **keine gesetzlich zugewiesenen Aufgaben des behördlichen Datenschutzbeauftragten**:
  - Führung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO
  - Durchführung der Datenschutz-Folgenabschätzung, Art. 35 DSGVO
- Die **Datenschutz-Folgenabschätzung** ersetzt die bisherige Vorabkontrolle und ist deutlich umfangreicher: → schwer zu kategorisieren, viele offene Fragen: Wann liegt „hohes Risiko“ vor?

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.

Weitere Zentrale Änderungen sind u.a.

- **Pflichten für Auftrags(daten)verarbeiter** werden umfangreicher, u.a. müssen Auftrags(daten)verarbeiter auch ein Verzeichnis von Verarbeitungstätigkeiten führen.
- Bei zu ungenauer Beauftragung können Auftrags(daten)verarbeiter ebenfalls zu Verantwortlichen werden.

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 gegenüber Dritten, 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?**

- 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.

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?

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“*** als Erweiterung des Rechts auf Löschen (Bsp. Ausscheiden eines Mitarbeiters)
  - ***Recht auf Datenübertragbarkeit („Portabilität“)***

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
- **Gemeinsame Datenschutzbeauftragte**, Art. 37 Abs. 3 DSGVO
  - Für mehrere Behörden oder öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

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.

Meldepflichten bei „Datenpannen“

- Nach Art. 33 und 34 DSGVO müssen „Verletzungen des Schutzes personenbezogener Daten“
  - unverzüglich und möglichst **binnen 72 Stunden**
  - der Aufsichtsbehörde (= Landesbeauftragter für den Datenschutz) und
  - ggf. den Betroffenen gemeldet werden, wenn aus der Verletzung möglicherweise ein **hohes Risiko** für die persönlichen Rechte und Freiheiten entsteht.
  - Inhalt der Meldung bestimmt sich nach Art. 33 Abs. 3
  - **Schutzverletzungen sind nach Art. 33 Abs. 5 für die Behörde prüfbar zu dokumentieren**

Art. 36

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.

Handlungsempfehlungen

Welche Schritte sollten zur Umsetzung der EU-DSGVO bereits jetzt ergriffen werden (1)?

- Den Datenschutz in der Kommune / Behörde ernst nehmen!
- Sicherstellen, dass bei allen Einführungen neuer und Änderungen bestehender Systeme der Datenschutz einbezogen wird.
- Dem / der Datenschutzbeauftragten ausreichend Zeit und Möglichkeiten geben, um sich mit der EU-DSGVO hinreichend zu beschäftigen. Hierzu gehören:
  - *Teilnahme an Fortbildungen, Kongressen*
  - *Lesen von Fachliteratur, Newslettern, Blogs, etc.*
  - *Webinare, e-Learnings*

Welche Schritte sollten zur Umsetzung der EU-DSGVO bereits jetzt ergriffen werden (2)?

- **Datenschutzdokumentation:** wichtiger denn je (vgl. Art. 5 Abs. 2 EU-DSGVO)
- Konsequenz: Alle datenschutz-relevanten Dokumente **auf den aktuellen Stand bringen** (und bei der Gelegenheit mit Datum und Versionsnummer versehen). Dies gilt insbesondere für
  - *Netzwerkübersicht, Soft- und Hardwareübersicht*
  - *(Internes) Verfahrensverzeichnis*
  - *Datenschutzkonzept, -handbuch*
  - *Datenschutzrichtlinien inkl. Dokumentation der Verantwortlichkeiten*
  - *Dokumentation angemessenen Schutzniveaus nach Stand der Technik (Maßnahmen nach Art. 7 BayDSG oder mehr?)*

Handlungsempfehlungen

Welche Schritte sollten zur Umsetzung der EU-DSGVO bereits jetzt ergriffen werden (3)?

- Sicherstellen, dass
  - die **Verfahrensübersicht aktuell und vollständig** ist
  - vorhandene TOM Art. 32 Abs. 1 DSGVO entsprechen
  - die vorhandenen Datenschutzerklärungen und **Einwilligungen korrekt formuliert** (Art. 13 und 14 DSGVO)
  - für alle Auftrags(daten)verarbeitungen **aktuelle und rechtskonforme ADV-Vereinbarungen** vorliegen - aktuelle Aufstellung als Tabelle, in einer Datenbank oder in einem DS-Management-System vorhanden?

Handlungsempfehlungen

Welche Schritte sollten zur Umsetzung der EU-DSGVO bereits jetzt ergriffen werden (4)?

- Sensibilisierung von Behördenleitung und Beschäftigten
- Ein (internes oder externes) Datenschutzaudit durchführen, um zu wissen, auf welchem Stand sich die Umsetzung des Datenschutzes bei Ihrer Behörde befindet, insbes. Satzungsrecht auf eventuellen Anpassungsbedarf hin überprüfen
- Festlegung der zeitlichen Abläufe und Verantwortlichkeiten in Bezug auf die Umsetzung und Rollen
- Vorgehen bei „Datenpannen“ festlegen

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.

RSS Datenschutzerklärung Impressum

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

Bürger
Verwaltung
Unternehmen
Presse
Landesbeauftrag-
ter

Datenschutzreform
2018

Aktuelles
Auskunftsanspruch
Häufige Fragen
Themen
Zuständigkeiten
Veröffentlichungen

Tätigkeitsberichte
Konferenzen
Recht & Normen

Sie sind hier: > Start > Datenschutzreform 2018

Datenschutzreform 2018

- Pressemitteilung: Datenschutzreform 2018
- Vorbemerkung zur Informationsreihe "Datenschutzreform 2018"
- Die Datenschutz-Grundverordnung (DSGVO) - Ein Überblick: Teil 1: Geltung und Anwendungsbereich
- Die Datenschutz-Grundverordnung (DSGVO) - Ein Überblick: Teil 2: Begriffe und Grundsätze
- Die Datenschutz-Grundverordnung (DSGVO) - Ein Überblick: Teil 3: Die rechtmäßige (Weiter-)Verarbeitung personenbezogener Daten
- Die Datenschutz-Grundverordnung (
  arbeiter und Datenschutzbeauftragt
- Die Einwilligung nach der Datenschu
- Der Sozialdatenschutz unter Geltun
- Der Gesetzentwurf zum neuen Baye

LMU Rechtsinformatikzentrum

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

EU-Datenschutz-Grundverordnung

DSK Datenschutzkonferenz

Die Datenschutzkonferenz (DSK) veröffentlicht seit Juli 2017 Auslegungshilfen zur Datenschutz-Grundverordnung (DS-GVO). In diesen Kurzpapieren werden unter den deutschen Aufsichtsbehörden abgestimmte einheitliche Sichtweisen zu verschiedenen Kernthemen der DS-GVO wiedergegeben. Die in den Papieren enthaltenen Auffassungen stehen unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung durch den Europäischen Datenschutzausschuss.

Die Kurzpapiere des BayLDA, die bereits seit Juni 2016 in regelmäßigen Abständen erschienen sind, können ebenso heruntergeladen werden.

DSK-Kurzpapiere zur DS-GVO:

1. Verzeichnis von Verarbeitungstätigkeiten
2. Aufsichtsbefugnisse/Sanktionen
3. Verarbeitung personenbezogener Daten für Werbung

BayLDA-Kurzpapiere zur DS-GVO:

1. Veröffentlichung zum Art. 32 DS-GVO - Sicherheit der Verarbeitung
2. Art. 42 DS-GVO - Zertifizierung
3. Videoüberwachung nach der DS-GVO - ein Ausblick
4. Recht auf Löschung ("Vergessenwerden") - Art. 17 DS-GVO
5. Verzeichnis von Verarbeitungstätigkeiten - Art. 30 DS-GVO
6. Besondere Kategorien personenbezogener Daten - Art. 9 DS-GVO
7. Sanktionen nach der DS-GVO
8. Umgang mit Datenpannen - Art. 33 und 34 DS-GVO
9. Einwilligungen nach der DS-GVO
10. Auftragsverarbeitung nach der DS-GVO
11. Datenübermittlungen in Drittstaaten nach der DS-GVO
12. Verarbeitung personenbezogener Daten für Werbung
13. One Stop Shop
14. Amtshilfe und gemeinsame Maßnahmen der Aufsichtsbehörden
15. Einwilligung eines Kindes
16. Auskunftsrecht der betroffenen Person
17. Verhaltensregeln - Art. 40 DS-GVO
18. Datenschutz-Folgenabschätzung (DSFA) - Art. 35 DS-GVO
19. Der Datenschutzbeauftragte (DSB) - Art. 37 bis 39 DS-GVO
20. Beschäftigtendatenschutz nach der DS-GVO und dem BDSG-neu

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

Kontakt zum Referenten

Bedarf an weiteren Informationen & Angeboten?

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