Aktuelles zu Prüfergebnissen einer Datenschutzaufsichtsbehörde im medizinischen Bereich

Andreas Sachs / Wiesbaden, 23. September 2019

Andreas Sachs

ist Informatiker, Bereichsleiter „Cybersicherheit & Technischer Datenschutz“ und Vizepräsident beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) in Ansbach.

Einige Schwerpunktthemen (unter DS-GVO)

Datenpannen & Hacking

Trackingverfahren

Privacy by Design

Automotive

IT-Sicherheit

Datenschutzfolgenabschätzung

Verschlüsselungsverfahren

Zertifizierung

Rechenschaftspflicht

Agenda

Prüfung der Umsetzung der DS-GVO (Datenschutz-Compliance)

- Aufbau- und Ablauforganisation
- Datenschutzbeauftragter
- Datenschutzkonforme Verarbeitung
- Umgang mit Betroffenenrechten
- Meldung von Datenschutzverletzungen

Prüfungen im medizinischen Bereich

- Ransomware in Arztpraxen
- Tracking auf Webseiten
- Windows 10 (im weitesten Sinne)
- Löschen von Daten

Paradigmenwechsel: Rechenschafts- und Nachweispflicht

Art. 5. Abs. 2 DSGVO
Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung **nachweisen** können („Rechenschaftspflicht“).

Datenschutzaufsichtsbehörde

Wird die DSGVO eingehalten? →

← Nachweis der Einhaltung

Verantwortlicher (DSGVO)

Rechenschaftspflicht: Bestandteil der Grundsätze

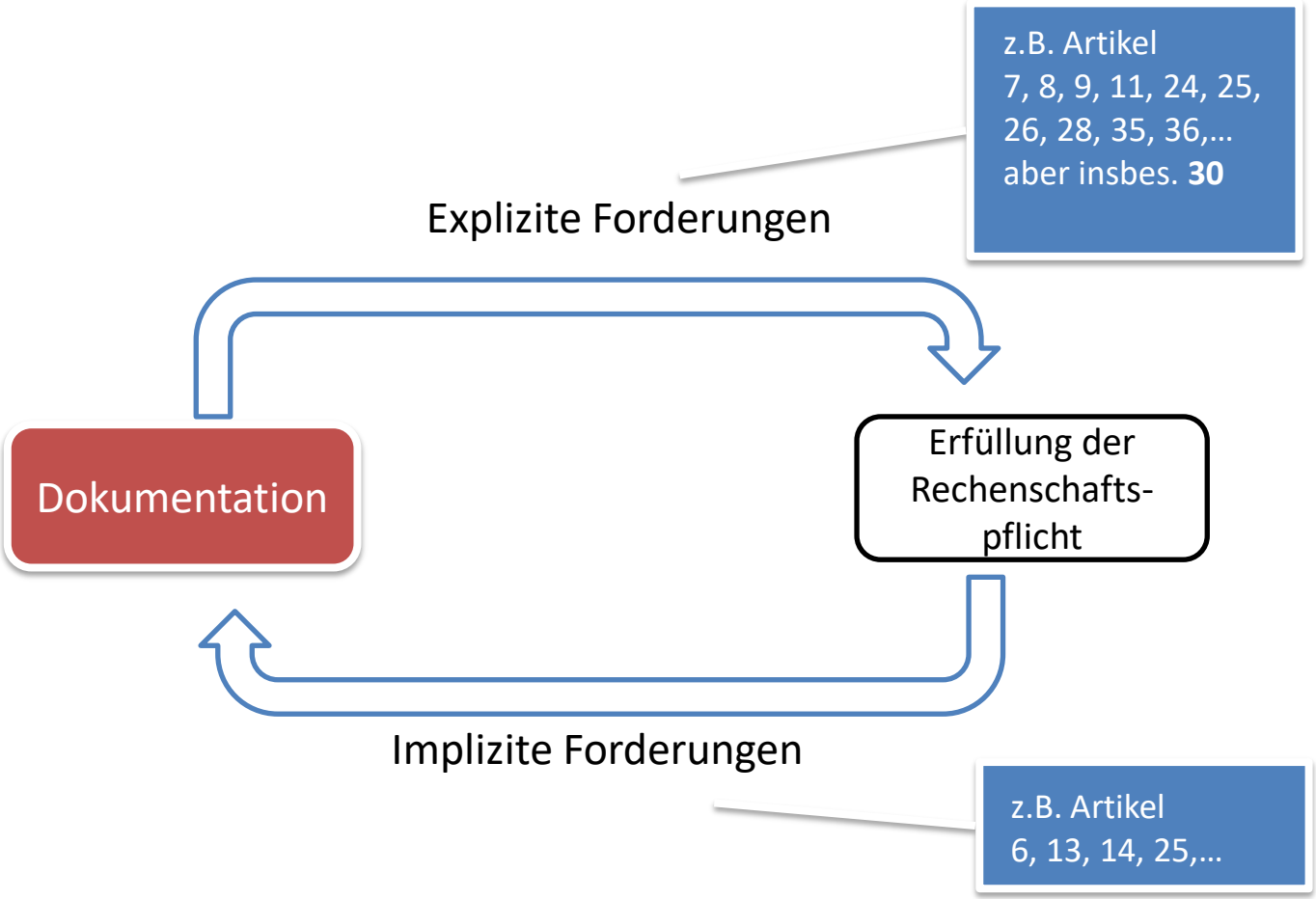
Art. 5: Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen
- a) … auf rechtmäßige Weise … („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“)
- b) … für festgelegte, eindeutige und legitime Zwecke … („Zweckbindung“)
- c) … auf das notwendige Maß beschränkt … („Datenminimierung“)
- d) … sachlich richtig … („Richtigkeit“)
- e) … erforderlich … („Speicherbegrenzung“) [und mit]
- f) … angemessener Sicherheit … („Integrität und Vertraulichkeit“)

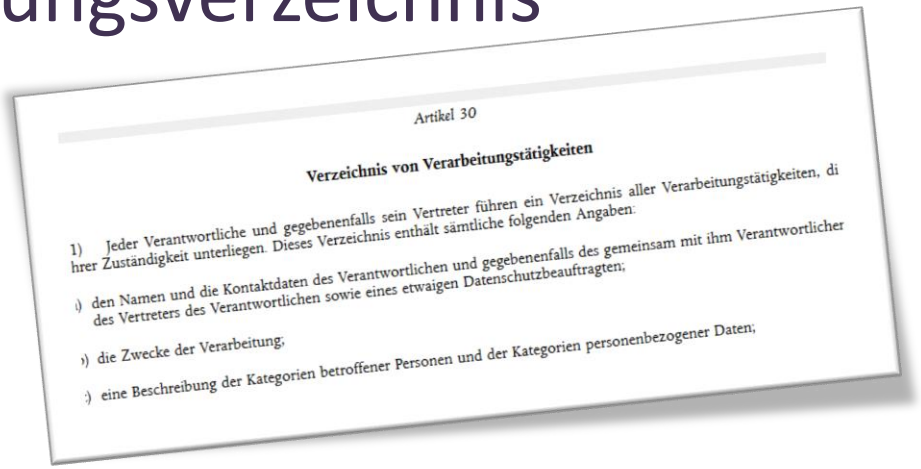
[verarbeitet werden.]

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Elemente der Rechenschaftspflicht



Zentral: Verarbeitungsverzeichnis



Artikel 30

Verzeichnis von Verarbeitungstätigkeiten

1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, di hrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

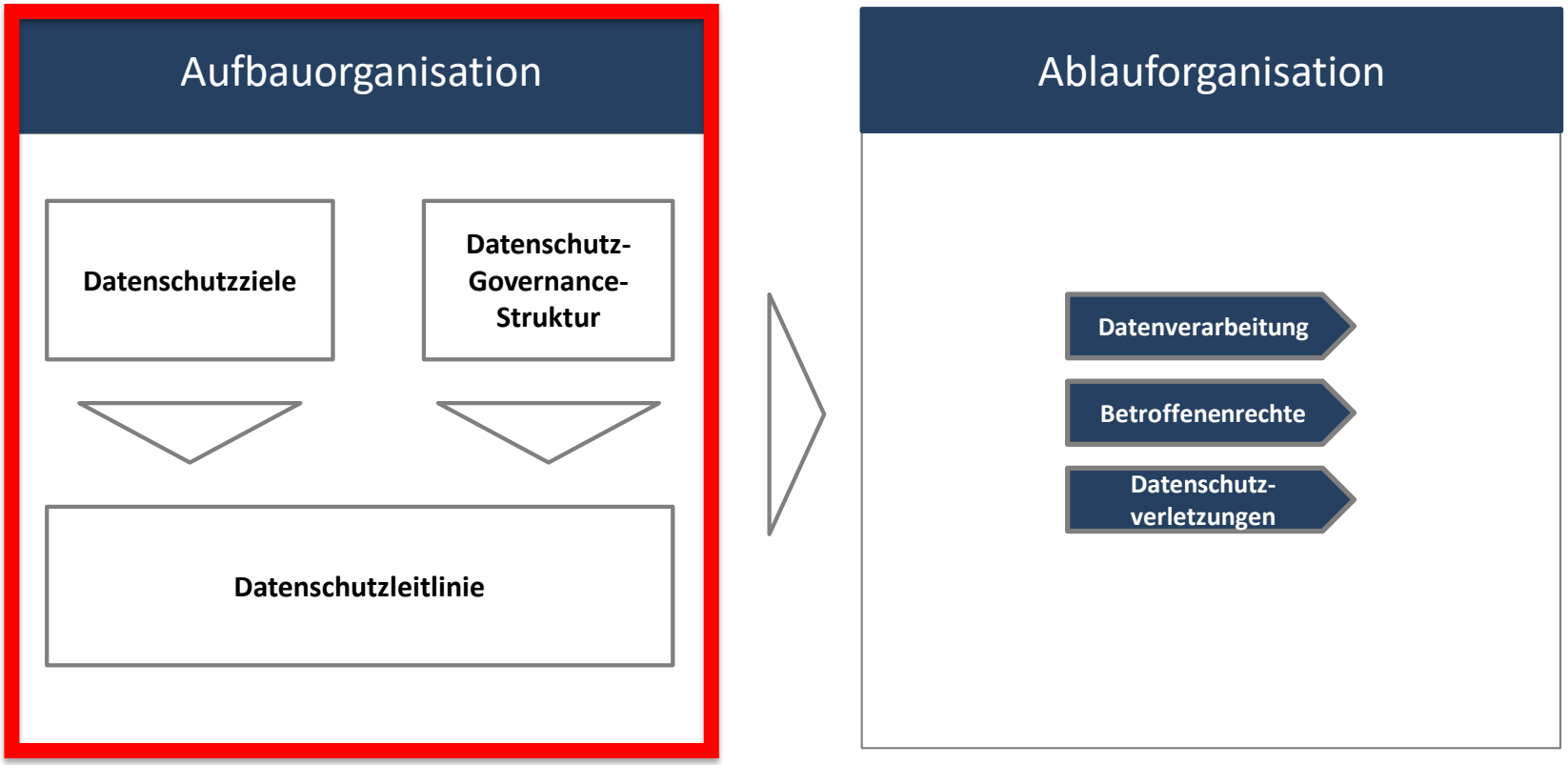
) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlicher des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

) die Zwecke der Verarbeitung;

) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

- Gehört zu den **Pflichten** der Verantwortlichen und Auftragsverarbeiter (Kapitel IV DS-GVO)
- Fokus: **Verarbeitungstätigkeiten**
- Es ist ein Verzeichnis aller Verarbeitungstätigkeiten **schriftlich** zu führen (auch elektronisch möglich)
- Verzeichnis wird der **Aufsichtsbehörde** auf Anfrage zur Verfügung gestellt

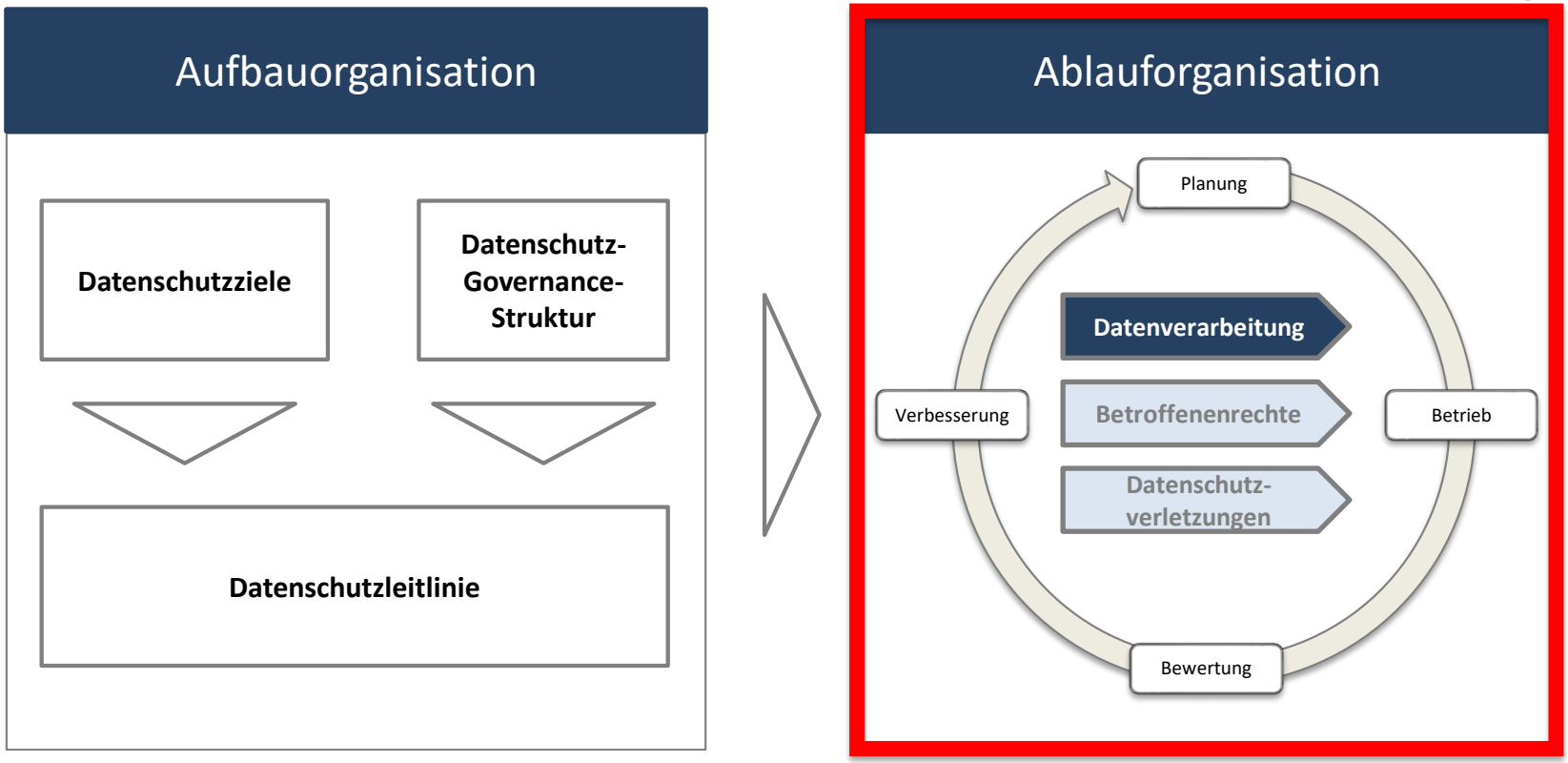
Was ist umfasst die Datenschutz-Governance?



Rechenschaftspflicht, Verantwortung des Verantwortlichen (Art. 5 Abs. 2, Art. 24)

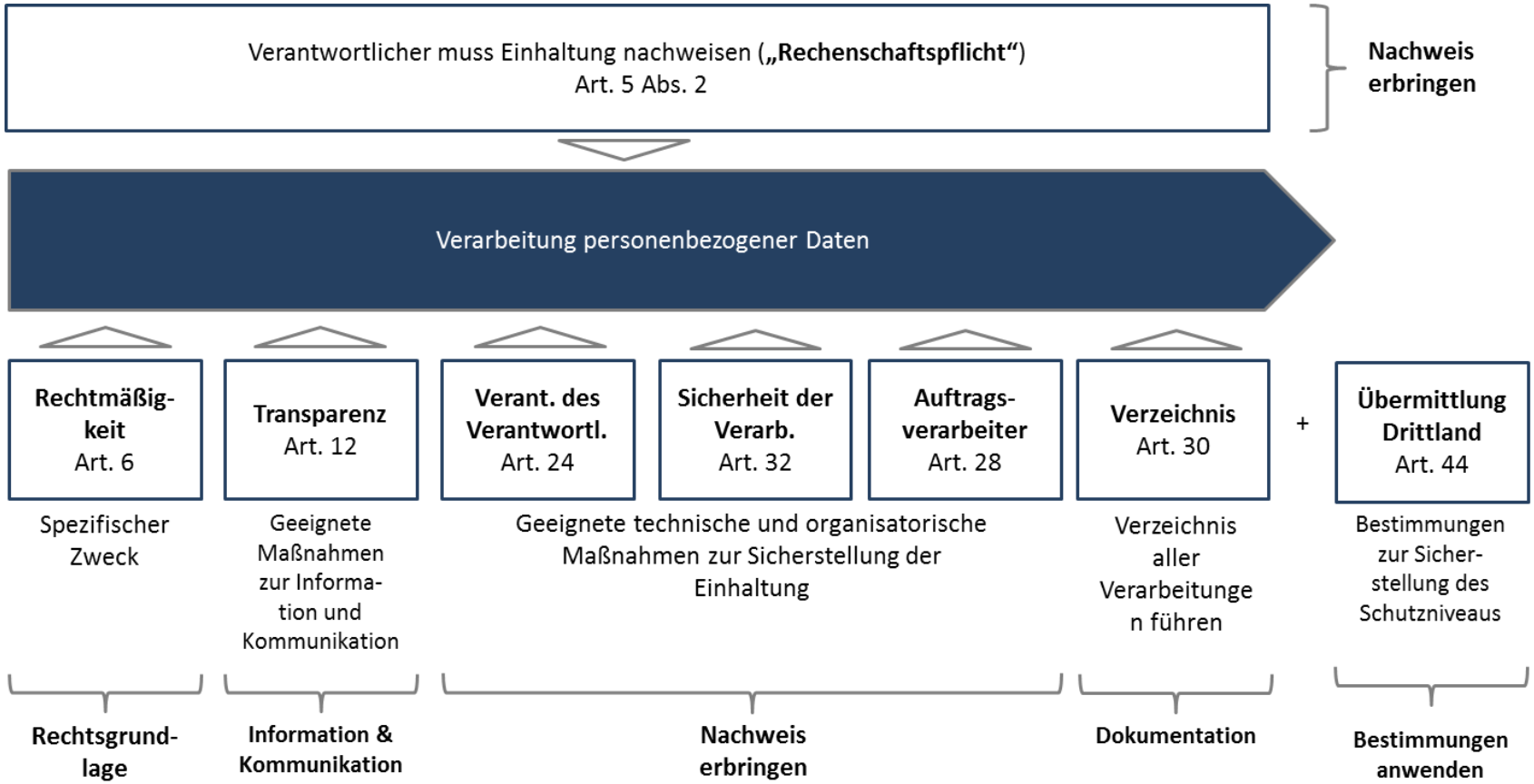
Quelle: Kranig / Sachs / Gierschmann,
Datenschutz-Compliance nach der DS-GVO, 2. Auflage 2019 (bald verfügbar)

Was umfasst die datenschutzkonforme Verarbeitung?



Einer der drei Datenschutz-Kernprozesse basierend auf dem PDCA-Zyklus

Voraussetzungen der datenschutzkonformen Verarbeitung



Was umfasst die Sicherstellung der Betroffenenrechte?

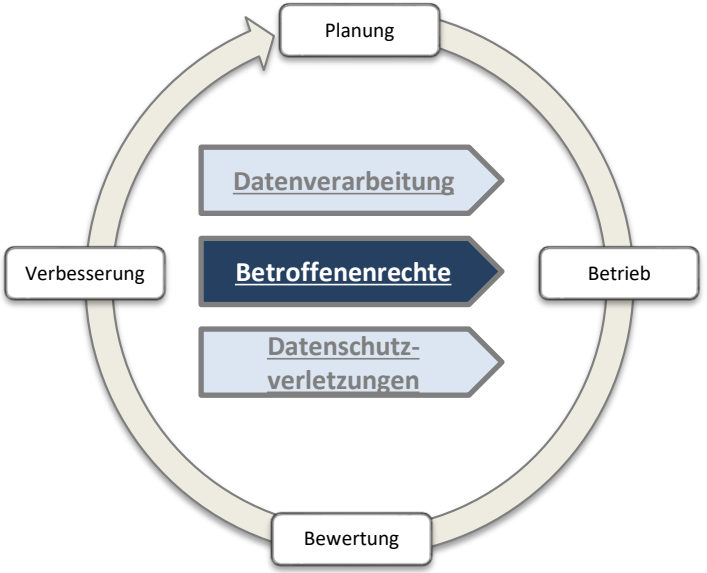
Aufbauorganisation

Datenschutzziele

Datenschutz-Governance-Struktur

Datenschutzleitlinie

Ablauforganisation



Einer der drei Datenschutz-Kernprozesse basierend auf dem PDCA-Zyklus

Quelle: Kranig / Sachs / Gierschmann,
Datenschutz-Compliance nach der DS-GVO, 2017

Überblick über Betroffenenrechte nach der DS-GVO

Transparente Information, Kommunikation und Modalitäten
Art. 12

Auskunft
Art. 15

Berichtigung, Löschung, Einschränkung
Art. 16 - 19

Datenübertragbarkeit
Art. 20

Widerspruch
Art. 21

Automatisierte Entscheidungen
Art. 22

Widerruf der Einwilligung
Art. 7 Abs. 3

Quelle: Kranig / Sachs / Gierschmann,
Datenschutz-Compliance nach der DS-GVO, 2017

Einzelfragen zum Recht auf Auskunft

- **Auskunft muss sich beziehen auf:**
  - Verarbeitungszwecke
  - Kategorien personenbezogener Daten
  - Empfänger oder Kategorien von Empfängern
  - Speicherdauer, mindestens Kriterien für Speicherdauer
  - Beschwerderecht bei Aufsichtsbehörde
  - Information über Herkunft der Daten
  - Wenn automatisierte Entscheidungsfindung: involvierte Logik
  - Wenn Übermittlung in Drittland: Info über geeignete Garantien
- **Frist für Auskunft:**
  - Unverzüglich
  - Jedenfalls innerhalb eines Monats
  - Verlängerung um zwei Monate bei Komplexität
- **Form der Auskunft:**
  - Kopie der personenbezogenen Daten (erste Kopie kostenlos)

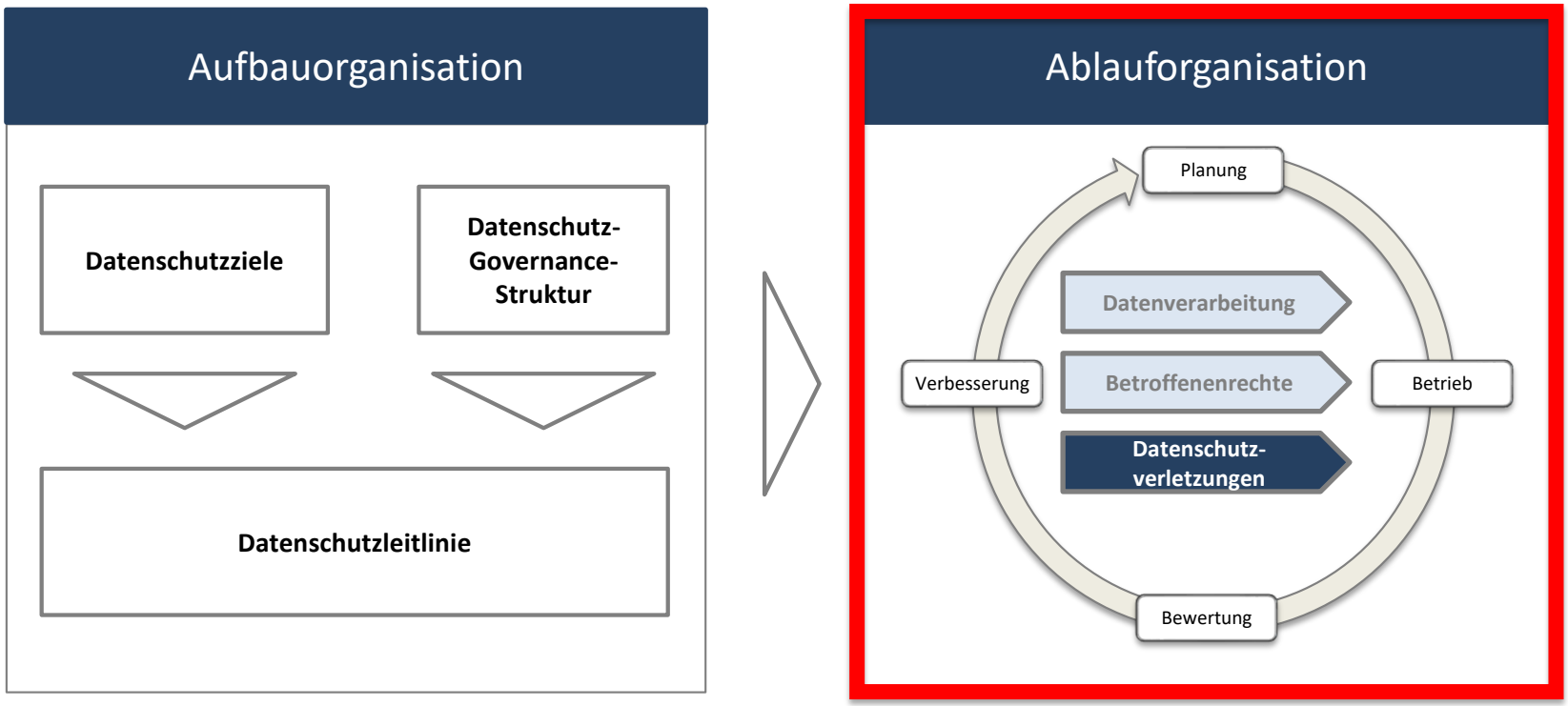
Verstoß: 20 Mio. EUR oder 4%

Diskussion:
Wie detailliert muss die Auskunft sein?

Prüfpraxis der Aufsichtsbehörden
Informationspflichten in Bewerbungsverfahren

Hier sollte der Prüfkatalog stehen

Was umfasst die Handhabung von Datenschutzverletzungen?



Einer der drei Datenschutz-Kernprozesse basierend auf dem PDCA-Zyklus

Umgang mit Datenschutzverletzungen

Working Paper 250
Beschäftigt sich mit Verletzungen der Sicherheit

ARTIKEL-29-DATENSCHUTZGRUPPE

18/DE

WP250rev.01

Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679

angenommen am 3. Oktober 2017

zuletzt überarbeitet und angenommen am 6. Februar 2018

Datenschutzverletzung – was ist das?

- Eine Verletzung des Schutzes personenbezogener Daten (kurz „Datenschutzverletzung“) ist gemäß Art. 4 Nr. 12 eine **Verletzung der Sicherheit**, die
  - ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust oder zur Veränderung (**Verlust der Verfügbarkeit bzw. Integrität**) oder
  - zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten (**Verlust der Vertraulichkeit**) führt.

Rahmenbedingungen für Meldung an Aufsichtsbehörde

- **Frist**: „unverzüglich und möglichst binnen 72 Stunden“
- **Inhalt**:
  - Kontaktdaten DSB
  - Beschreibung von: (Ergänzung möglich)
    - Art der Verletzung,
    - Kategorien, Anzahl Personen und Datensätze
    - Wahrscheinliche Folgen der Verletzung
    - Vom Verantwortlichen ergriffene bzw. geplante Maßnahmen
- **Dokumentation** der Verletzung

Rahmenbedingungen für die Erfüllung der Benachrichtigungspflicht gegenüber betroffenen Personen

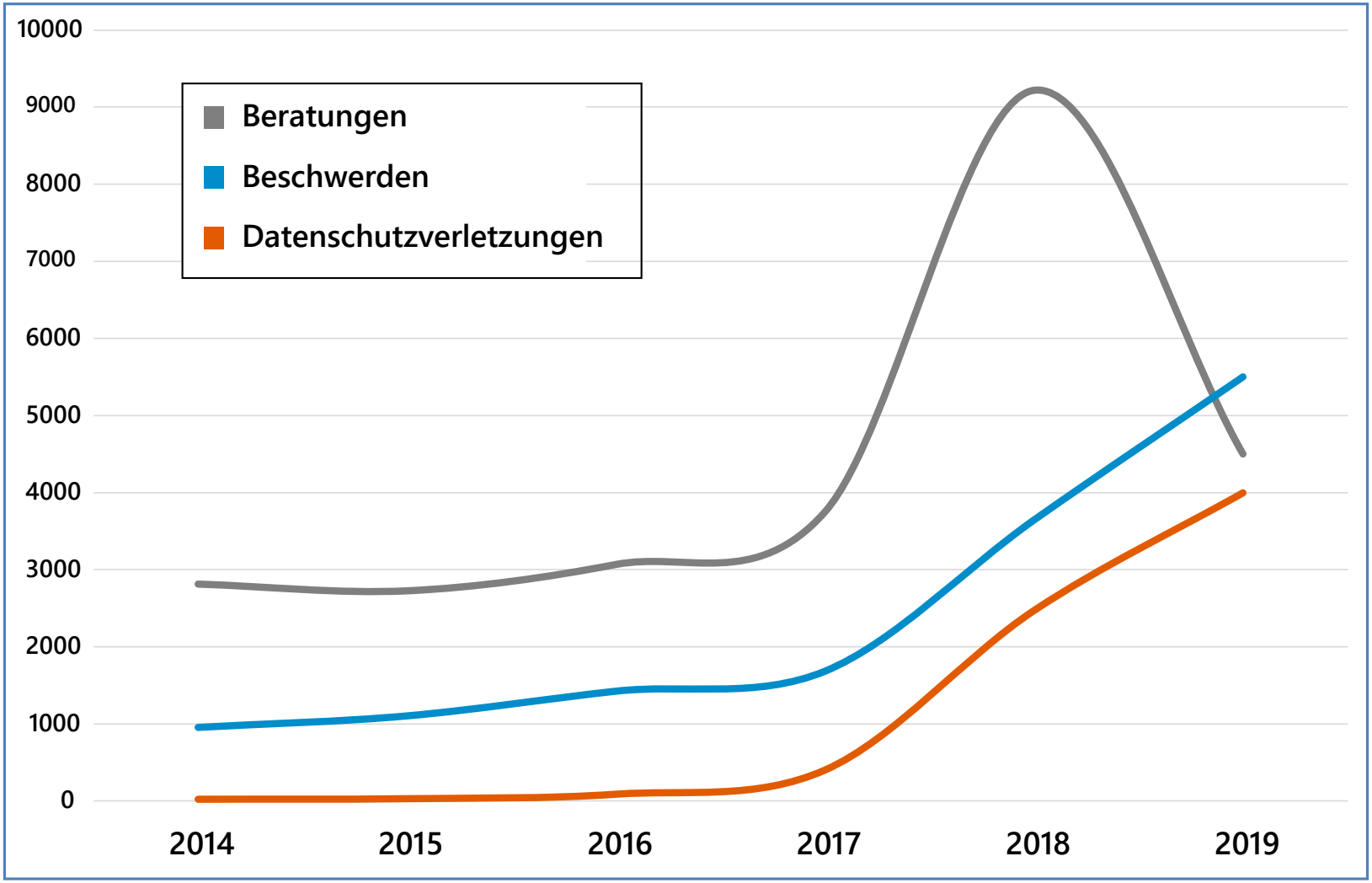
- **Voraussetzung:** Hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen
- **Frist**: unverzüglich
- **Inhalt**: (*in klarer und einfacher Sprache*)
  - Beschreibung von:
    - Art der Verletzung,
    - Name und Kontaktdaten DSB
    - Wahrscheinliche Folgen der Verletzung
    - Vom Verantwortlichen ergriffene bzw. geplante Maßnahmen

Handhabung von Datenschutzverletzungen

- **Vorbereitung auf Meldung wegen Datenschutzverletzungen**

  - ErwGr. 87: *Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können.*

  - Daraus folgt: Pflicht zur Vorbereitung auf Datenschutzverletzungen!


10000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
Beratungen
Beschwerden
Datenschutzverletzungen
2014
2015
2016
2017
2018
2019

Einblick in aktuellen Themen und Prüfungen

Ransomware in Arztpraxen

?

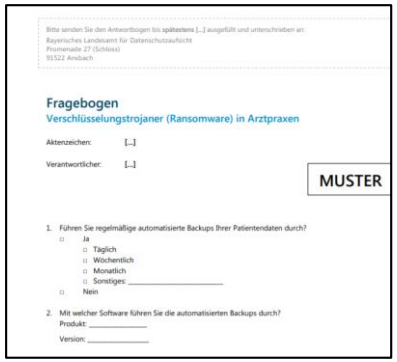
Ransomware in Arztpraxen

- Schutzmaßnahmen nach Art. 32 erforderlich
- Bei einem Vorfall:
  - Art. 33 – Risiko der Rechte und Freiheiten
  - Art. 34 – Hohes Risiko der Rechte und Freiheiten
- Meldungen nach Art. 33 bei der Aufsichtsbehörde
  - Seit 01.01.2019 ca. 90 Meldungen
- Ziel der Prüfung:
  - Awareness-Schutzmaßnahmen
  - Netztrennung
  - Funktionierende Backups

Informationen zur Prävention/Reaktion bezügl. Schadcode-Befall:
https://www.lda.bayern.de/schadcode

Ransomware in Arztpraxen

Fragebogen zum Selbsttest:
https://www.lda.bayern.de/media/pruefungen/201810_ransomware_fragebogen.pdf



Bitte senden Sie den Antwortbogen bis spätestens [...] ausgefüllt und unterschrieben an:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 (Schloss)
91522 Ansbach

Fragebogen
Verschlüsselungstrojaner (Ransomware) in Arztpraxen

Aktenzeichen: [...]

Verantwortlicher: [...]

MUSTER

1. Führen Sie regelmäßige automatisierte Backups Ihrer Patientendaten durch?
   - ☐ Ja
     - ☐ Täglich
     - ☐ Wöchentlich
     - ☐ Monatlich
     - ☐ Sonstiges: _____
   - ☐ Nein
2. Mit welcher Software führen Sie die automatisierten Backups durch?
   Produkt: _____
   Version: _____

Infoblatt:
https://www.lda.bayern.de/media/pruefungen/201810_ransomware_info.pdf

Bayerisches Landesamt für Datenschutzaufsicht

Informationsblatt

Verschlüsselungstrojaner (Ransomware) in Arztpraxen

1. *Führen Sie regelmäßige automatisierte Backups Ihrer Patientendaten durch?*
   Regelmäßige Backups sind wichtig, um die Verfügbarkeit der Patientendaten sicherzustellen. Im Falle einer Verschlüsselung der Daten durch Schadsoftware, können die Daten aus aktuellen Backups schnell wiederhergestellt werden und somit kann auch die Beeinträchtigung der Betroffenen minimiert werden.
2. *Mit welcher Software führen Sie die automatisierten Backups durch?*
   Eine geeignete Software in einer aktuellen Version kann die Erstellung automatisierter Backups erleichtern. Solch eine Software hilft aber auch bei der Wiederherstellung der Daten im Falle eines Datenverlustes.
3. *Auf welchen Speichermedien werden die Backups gespeichert?*
   Wichtig bei der Auswahl des Speichermediums ist, dass die erstellten Backups getrennt von den entsprechenden Rechnern liegen. Nur so ist im Falle eines Verschlüsselungstrojaners sichergestellt, dass nicht auch

Tracking auf medizinischen Webseiten

27. August 2019, 4:49 Uhr Bayerisches Rotes Kreuz

Blutspendedienst übermittelte heikle Daten an Facebook

Der Blutspendedienst des BRK sammelt Blutspenden - und verteilt dabei allem Anschein nach auch Daten von Nutzern seiner Webseite, die sich nur informieren wollen. (Foto: Arno Burgi)

Tracking auf medizinischen Webseiten

27. August 2019, 4:49 Uhr Bayerisches Rotes Kreuz

Blutspendedienst übermittelte heikle Daten an Facebook

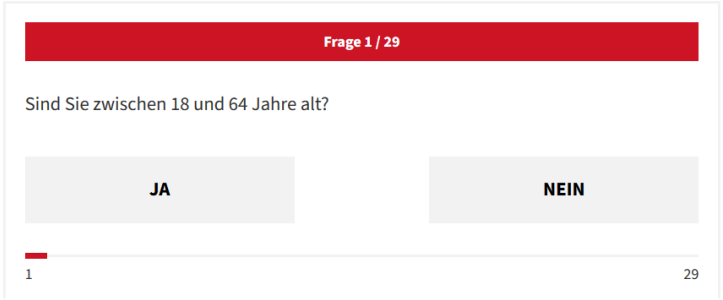
Der Blutspendedienst des BRK sammelt Blutspenden - und verteilt dabei allem Anschein nach auch Daten von Nutzern seiner Webseite, die sich nur informieren wollen. (Foto: Arno Burgi)

Tracking auf medizinischen Webseiten

Spende-Check

Sicherheit für Spender und Transfusionsempfänger haben höchste Priorität. Um diesem Anspruch gerecht zu werden, gibt es gute Gründe, einen Spender zeitweise oder dauerhaft von der Blutspende auszuschließen.

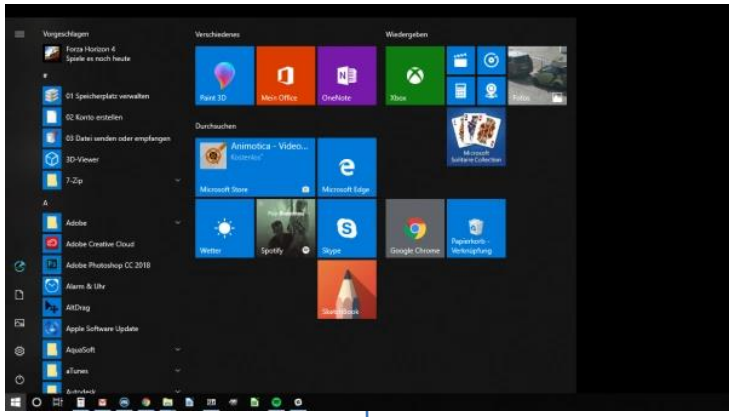
Mit unserem Spende-Check finden Sie in wenigen Schritten heraus, ob Sie derzeit zur Spende zugelassen werden können oder nicht. Die letztendliche Entscheidung über Ihre Spendefähigkeit obliegt dem diensthabenden Arzt beim Spendetermin.



Haben oder hatten Sie jemals eine schwere Erkrankung (z. B. Herzerkrankungen wie Herzinfarkt oder Herzkranzgefäßerkrankung, Bypass-Operation, Aufweiten einer Herzkranzarterie, Setzen von Stents; neurologische Erkrankungen wie Schlaganfall oder sonstige Durchblutungsstörungen des Gehirns – auch in der Vergangenheit)?

Einsatz von Windows 10

Kann ich dies überhaupt einsetzen?



Telemetrie

Einsatz von Windows 10

Auftrag

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

-

Positionierung der DSK zum datenschutzkonformen Einsatz von Windows 10

Datenschutzrisiken moderner Betriebssysteme wurden bereits mehrfach in der DSK beraten. Die 90. DSK hat im Herbst 2015 die Entschließung zu Cloud-unterstützten Betriebssystemen verabschiedet.

Die DSK hat sich entschlossen, dem Arbeitskreis Technik den Auftrag zu erteilen, eine datenschutzrechtliche Positionierung zum Einsatz von Windows 10 zu erarbeiten und diese zur Grundlage eines weitergehenden, vom LDA Bayern zu koordinierenden Dialoges mit Microsoft zu datenschutzrechtlichen Fragestellungen zum Produkt Windows 10 zu machen.

Einsatz von Windows 10

Windows-10-Editionen im Vergleich			
	Home	Pro	Enterprise

SiSyPHuS Win10 Studie dies Bundesamt für Sicherheit in der Informationstechnik
(https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html)

Datenschutzfolgenabschätzung zu Windows 10 des Niederländisches Justizministeriums
(https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/DPIA+Windows+10+version+1.5+11+June+2019.pdf)

Dauerbrenner: Löschen von Daten

https://www.sueddeutsche.de/digital/datenschutz-verdacht-auf-unzulaessig-gespeicherte-kundendaten-in-apot

München 22°

Süddeutsche Zeitung

Shop Jobs Immobil

SZ.de Zeitung Magazin

Politik Wirtschaft Meinung Panorama Sport München Bayern Kultur Gesellschaft Wissen Digital Karriere Reise Auto

Home > Digital > Digitale Privatsphäre > Apotheken: Verdacht auf unzulässig gespeicherte Daten

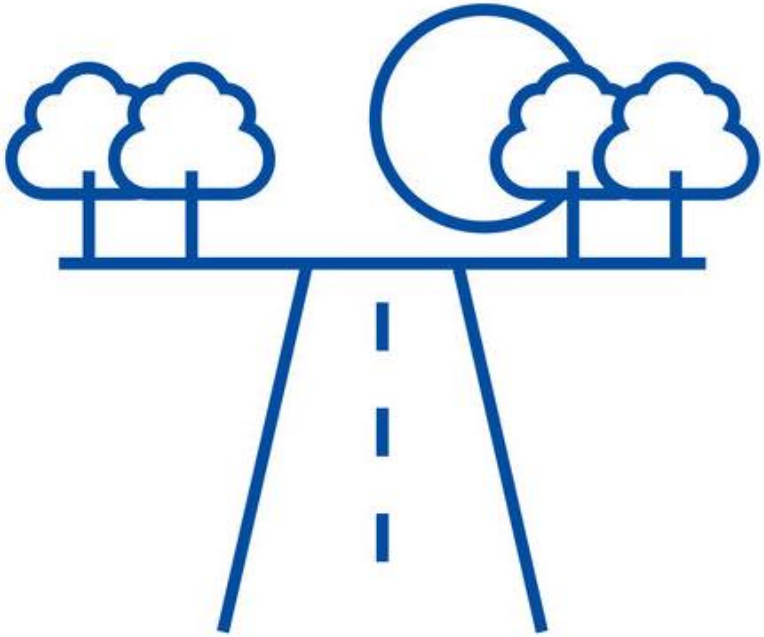
Internet-Si

20. Dezember 2018, 18:33 Uhr Datenschutz

Verdacht auf unzulässig gespeicherte Kundendaten in Apotheken

- Apotheker setzen Software ein, um Rezepte zu erfassen. Einer der größten Software-Hersteller erfasst dabei möglicherweise mehr Daten als erlaubt ist.
- Es ist ein Vorwurf, dem nun das Bayerische Landesamt für Datenschutzaufsicht nachgeht.
- Der Hersteller weist alle Schuld von sich. Es komme "ein abgestuftes

Welche weiteren Themen sind am Horizont erkennbar



- Orientierungshilfe Email-Verschlüsselung
- Anforderungen an Messenger-Dienste im Krankenhaus
- Prüfung der PACS-Systeme (In Vorbereitung)
- Standard-Datenschutzmodell Version 2.0
- Zertifizierung nach DS-GVO wird (hoffentlich) 2020 kommen

Vielen Dank für Ihre Aufmerksamkeit