SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz

Die Datenschutz-Grundverordnung aus Sicht einer Aufsichtsbehörde
Erfahrungen – Empfehlungen – Rechtsentwicklungen

Dr. Harald von Bose

Agenda

- Eckdaten DS-GVO (Ziele, Anwendung, Evaluierung)
- Arbeitsweise der Aufsichtsbehörden (Beschwerden, Anfragen, grenzüberschreitende Zusammenarbeit, Beratungen)
- Irrtümer, Ängste
- Umsetzung in KMU
- Rechtsfolgen von Verstößen (Verwarnungen, Verbote, Bußgelder)
- KI, neue Geschäftsmodelle

Ziele der DS-GVO

- Harmonisierung, gleichmäßig hohes Datenschutzniveau (vgl. Erwägungsgrund 13)
  - ein **einheitliches Datenschutzrecht** für in der EU tätige Unternehmen (inkl. Marktortprinzip)
  - kein „Forum-Shopping“ möglich (Datenverarbeitung in Mitgliedstaat mit geringstem Datenschutzniveau)
  - „One-Stop-Shop“; **konzentrierte Zuständigkeit** der Aufsichtsbehörden (federführende Aufsichtsbehörde am Hauptsitz von Unternehmen)
  - Stärkung des Binnenmarktes
- Modernisierung (Berücksichtigung Globalisierung / Internet / Big Data, Wirtschaft 4.0)

Anwendung der DS-GVO

- Seit dem 25. Mai **2016**: DS-GVO **in Kraft**
- Seit dem 25. Mai **2018**: DS-GVO **anzuwenden (Kernartikel: 6 – 5 – 25/32)**

- **Evaluierung**
  Bis zum 25. Mai 2020 legt EU-Kommission dem Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung der DS-GVO vor (Art. 97 DS-GVO).

  Schwerpunkt der EU-Kommission: Beachtung der DS-GVO im nationalen Recht der Mitgliedstaaten

Tätigkeit des Landesbeauftragten in Sachsen-Anhalt

…ist seit Geltung der DS-GVO insbesondere geprägt durch

- Beschwerden und Eingaben (358*)
- Informationen und Beratungen (789*)
- Meldungen von Datenschutzverletzungen (53*)
- Abhilfebefugnisse inkl. Bußgeldverfahren
- Kooperation und Kohärenz gem. Art. 56, 60 ff. DS-GVO
- förmliche Begleitung von Rechtsetzung (Bundes- u. Landesrecht, Ergänzungen und Umsetzungen von DS-GVO und JI-Richtlinie)
- Mitwirkung an Leitlinien u. a. des EDSA über DSK

*) die Zahlen beziehen sich auf den Zeitraum vom 15.06.2018 – 31.12.2018, Tendenz für 2019: in etwa gleichbleibend, bei Meldungen steigend

Inhalte der Beschwerden, Eingaben, Beratungen (1)

…sind auch abhängig von der Wirtschaftsstruktur

In Sachsen-Anhalt

- Wenig Hauptniederlassungen/Firmensitze großer Unternehmen/Konzerne
- Aber: viele Filialen/Produktionsstätten, mitunter mit eigener Entscheidungsbefugnis in Datenschutzbelangen
- Viele KMU
- Insgesamt ca. 74.000 Unternehmen mit sozialversicherungs-pflichtig Beschäftigten und / oder steuerbarem Umsatz
  (Quelle: Statistisches Landesamt Sachsen-Anhalt)
- Personal LfD: 20 Stellen für Datenschutz, davon 7,5 Stellen nöB ☹

Inhalte der Beschwerden, Eingaben, Beratungen (2)

- **Schwerpunkte von Anfragen**
  - Benennungspflicht von Datenschutzbeauftragten (hätten die Fragen schon nach altem Recht gestellt werden müssen?)
  - Erfüllung von Betroffenenrechten, insbes. der Informationspflichten sowie der Ansprüche auf Auskunft und Löschung
  - Kunden- und Beschäftigtendatenschutz, Schutz von Gesundheitsdaten
  - Techn. und org. Maßnahmen (z. B. Risikobewertung, Auftragsverarbeitung bei Einschaltung von Dienstleistern, Verschlüsselung, technische Neuerungen/Trends)
- **Schwerpunkte von Beschwerden**
  - mangelnde oder keine Erfüllung von Betroffenenrechten, insbes. der Informationspflichten sowie der Ansprüche auf Auskunft und Löschung
  - Videoüberwachung
  - Kunden- und Beschäftigtendatenschutz, Schutz von Gesundheitsdaten
  - mangelnde Verschlüsselung

Sensibilisierung, Aufklärung, Beratung

- Rechtsgrundlagen:
  Art. 57 Abs. 1 lit. b, d, l, Art. 31 DS-GVO und § 40 Abs. 6 BDSG
- Formen:
  - Einzelberatungen
  - Einrichtung eines Arbeitskreises mit den Kammern
  - Informationsveranstaltungen in Zusammenarbeit mit Landesverbänden von Vereinen
  - Beteiligung an Arbeitskreisen von Datenschutz- und Unternehmensverbänden
  - Zusammenarbeit mit Verbraucherzentrale

Zusammenarbeit bei grenzüberschreitenden Fällen

- Art. 56, 60 ff. DS-GVO: Zusammenarbeit der Aufsichtsbehörden (wenn mehrere Niederlassungen in der EU oder Betroffene in mehreren Mitgliedstaaten)
  - Internetanwendung „Internal Market Information System“ (IMI) auf Englisch
  - Federführende AB an der Hauptniederlassung legt Beschluss vor, andere AB stimmen zu oder
  - streitiger Einspruch -> Verbindlicher Beschluss des EDSA (Art. 65 Abs. 1 a) DS-GVO)
- Vorab innerhalb D., Abgabe an deutsche (Haupt-)Niederlassung nach § 19 Abs. 2 BDSG
  - Beispiel: Beschwerde in ST gg. Unternehmen in Luxemburg (LU), Abgabe an AB im Bundesland der deutschen Niederlassung (BB), IMI, Federführende europäische AB (LU), Verfahren mit Unternehmen, Beschlussvorschlag, Abstimmung mit betroffenen AB (z.B. ST), ggf. Einspruch und Beschluss EDSA, Verfügung an das Unternehmen (LU)/ Beschwerdeantwort an Beschwerdeführer (BB-> Beschwerdeführer in ST)
- Kritik: Arbeitsaufwändiges, schwerfälliges Verfahren in IMI, unterschiedliche Verwaltungskulturen, keine proaktive Aufsicht über globale Internetkonzerne

Zusammenarbeit vs. Aussageverweigerung

- Verantwortliche müssen nach Art. 31 DS-GVO mit der AB zusammenarbeiten, indem sie u.a. Informationen bereitstellen (Art. 58 Abs. 1 lit. a) oder zuarbeiten (Art. 30 Abs. 4, 36, 37 Abs. 7, 42 Abs. 6, 49 Abs. 1 S. 2, 60 Abs. 10 DS-GVO)
- „Zwischen Skylla und Charybdis“: Diese Pflicht ist bußgeldbewehrt (Art. 83 Abs. 4 lit. a) DS-GVO), aber Offenlegung von Verstößen kann ebenfalls zu Bußgeldern führen
- Voraussetzung: Belehrung über Auskunftsverweigerungsrechte im Falle der Selbstbelastung nach § 40 Abs. 4 BDSG, auch zu Gunsten der juristischen Person (GF muss nicht die GmbH belasten)
- Sonst: Beweisverwertungsverbot nach Art. 6 Abs. 1 EMRK, 47 Abs. 2 S. 1 GRCh der EU (nemo tenetur)

- Spezialfall Datenpannenmeldung (Art. 33 DS-GVO): Gesetzliche Pflicht zur Meldung führt zum gesetzlichen Verwertungsverbot nach § 43 Abs. 4 BDSG [eng auslegen]

Bußgeldverfahren (1)

Art. 58 Abs. 2 lit. i DS-GVO: Einleitung eines Bußgeldverfahrens zusätzlich zu oder anstelle von einer verwaltungsrechtlichen Anweisung (Einzelfallbetrachtung)

Kriterien für das „Ob“ der Verfahrenseinleitung nach Art. 83 Abs. 2 DS-GVO, EG 148: Art, Dauer und Schwere des Verstoßes, dessen Auswirkungen, Verschuldensgrad des Verantwortlichen, Kooperation mit Aufsichtsbehörde

I.d.R. kein Bußgeldverfahren:
- bei geringfügigem Verstoß (dann ggf. Verwarnung)
- z. B. bei erstem, unabsichtlichen Verstoß eines Unternehmens, bei dem die Datenverarbeitung nur eine Nebentätigkeit ist
- z. B. wenn der Verstoß sofort nach Hinweis der Aufsichtsbehörde abgestellt wird (Beispiel: die mangelhafte Kennzeichnung einer ansonsten zulässigen Videoüberwachung in einem Wohnblock wird innerhalb weniger Tage durch ordnungsgemäße Beschilderung beseitigt)

Bußgeldverfahren (2)

Bußgeldhöhe: maßgeblich sind die Kriterien nach Art. 83 Abs. 2, EG 150 sowie der Unternehmensumsatz (vgl. Bußgeldkonzept der DSK) bzw. die wirtschaftlichen Verhältnisse einer natürlichen Person

Honoriert wird nach Art. 83 Abs. 2 S. 2 DS-GVO

- das frühzeitige Abstellen des Verstoßes (lit. c) (z.B. Auskünfte werden zwar verspätet, aber erteilt),
- der Umfang der frühzeitigen und aktiven Kooperation mit der Aufsichtsbehörde (lit. f) zur Minimierung nachteiliger Auswirkungen des Verstoßes, damit z.B. die Aufsichtsbehörde Untersuchungen/Schutzmaßnahmen veranlassen kann,
- der Umfang des Nachtatverhaltens -> Verbesserung der Datenschutzsicherheit,
- ggf. die Meldung des (nicht nach Art. 33 Abs. DS-GVO meldepflichtigen) Verstoßes, bevor eine Beschwerde bei der Aufsichtsbehörde eingeht (lit. h)

Verhängte Bußgelder: verspätete Auskunftserteilung: 2.300 €, unverschlüsselte E-Mail mit Gesundheitsdaten an falschen Empfänger: 3.700 €, Versand unzulässiger Werbe-E-Mails: 1.150 €, E-Mails mit umfangreichem offenen Verteiler: 2.500 €

Verbreitete Irrtümer/Ängste

- „Die Verarbeitung personenbezogener Daten erfordert **immer eine Einwilligung**, auch bei der Anfertigung von Fotos“
  Nein, bei Verträgen ist insbes. Art. 6 Abs. 1 S. 1 lit. b DS-DVO zu beachten, bei Fotos können die Wertungen des KUG in die Abwägungsentscheidung nach Art. 6 Abs. 1 lit. f) DS-GVO einfließen
- „Alle **Angehörigen eines Gesundheitsberufes** benötigen einen **Datenschutzbeauftragten**“
  Nein, siehe Beschluss DSK v. 26./27.04.2018, regelmäßig keine Benennungspflicht bei Kleinpraxen
- „Es bestehen immense flächendeckende **Abmahnrisiken**“
  Es gab einzelne Abmahnverfahren, aber keine Abmahnwelle
  Abmahnrisiko: Datenschutzerklärungen auf Homepages
  Gesetz zur Stärkung eines fairen Wettbewerbs: Entwurf BReg sieht vor, dass Anspruch des Abmahnenden u. a. entfällt bei Verstößen gegen die DS-GVO durch kleine Unternehmen (< 10 Beschäftigte sowie Jahresumsatz ≤ 10 Mio €) und vergleichbare Vereine

Datenverarbeitung durch KMU (1)

Beispiel: Augenoptikermeister mit 2 Filialen, 8 angestellten Optikern und 2 angestellten weiteren Meistern

Verarbeitungen:

- Kontakt- und Vertragsdaten in Papierform und auf PC
- Homepage mit Kontaktformular, z. B. für Terminabsprachen
- Computer mit Betriebssystem „Windows 7“ (läuft aus); Verwaltungsprogramm für den Optikerbetrieb (inkl. Fernwartung); elektronische Übermittlung an Hersteller, Krankenkassen und Abrechnungsstellen
- Telefonnummern der Kunden, Geschäftspartner und Beschäftigten auf Handy gespeichert, Nutzung von WhatsApp
- Kundendaten in (europäischer?) Cloud gespeichert, damit sie mobil abgerufen werden können (Chef ist viel unterwegs)
- wegen Diebstählen aus den offenen Brillenregalen läuft Videoüberwachung auch während der Öffnungszeiten mit Fernzugriff
- Personalverwaltung inkl. Lohnabrechnung (zumindest teilw. elektronisch, Übermittlungen an Steuerberater)

KMU: Datenschutzrechtliche Fragestellungen (2)

- Verarbeitungen auf das erforderliche Maß beschränkt?
- Informationspflichten erfüllt gegenüber Kunden und Besuchern der Homepage?
- Verfügt Rechner über aktuelle Software, Virenschutz, Firewall?
- Sind Server genügend abgesichert (Verfügbarkeit, Belastbarkeit…)
- Ist Vertrag über Auftragsverarbeitung für die Fernwartung der Verwaltungssoftware erforderlich, wenn ja, liegt vollständiger Vertrag nach Art. 28 Abs. 3 vor? Vertrag für Clouddienste?
- Sind diverse Datenübermittlungen nach aktuellem Stand der Technik verschlüsselt? Werden Übermittlungen auf das erforderliche Maß beschränkt?
- Ist Videoüberwachung auf das erforderliche Maß beschränkt, ist Fernzugriff abgesichert (Passwort und Verschlüsselung)?
- Sind Dokumentationspflichten erfüllt?

KMU: Verarbeitung mit Datenschutzkompetenz (3)

1. These: Der Betrieb bedarf der **datenschutzrechtlichen Kompetenz**, damit folgende häufig auftretende auch bußgeldrelevante Fehler vermieden werden: unzulässige Speicherung einzelner Kundendaten, keine Verschlüsselung des Kontaktformulars, Videoüberwachung unzulässiger Bereiche, mobiler Datenträger nicht verschlüsselt (bei Verlust: Meldung nach Art. 33), keine Erstellung des Verzeichnisses der Verarbeitungstätigkeiten, unzureichende Erfüllung Betroffenenrechte, fehlender Vertrag über Auftragsverarbeitung
2. These: **Lehrgangsinhalte** zur Vorbereitung auf die Meisterprüfung **reichen nicht aus** (für das gesamte Berufsrecht, Vertragsrecht, Arbeitsrecht sieht der Rahmenlehrplan der Augenoptiker 25-35 UStd. vor, darin enthalten: „wichtige Grundsätze des Datenschutzes“)
3. These: Es müssen **zusätzliche Kompetenzen** erworben werden, z. B. durch Schulungen der Mitarbeiter, externe Beratung, Branchenverbände oder idealerweise die (fakultative) Benennung eines Datenschutzbeauftragten, Art. 37 Abs. 4
4. These: Ein angemessenes **Datenschutzmanagement** ist unabdingbar!
5. Achtung: **Aufsichtsbehörden überwachen** Anwendung der DS-GVO auch in KMU!

Vorwurf: „unterschiedliche Auslegung der DS-GVO durch die Aufsichtsbehörden“

Zugegeben, Aufsichtsbehörden sind mitunter **unterschiedlicher Meinung**, u. a. bei den Fragen,

- ob bei der Übernahme der Patientenkartei durch Praxisnachfolger
- oder der Lohnbuchhaltung durch einen Steuerberater

ein Vertrag über eine **Auftragsverarbeitung** erforderlich sei.

Aber:

20 **Kurzpapiere** sowie zahlreiche **Beschlüsse** und **Entschließungen** (darunter auch Orientierungshilfen und Positionspapiere), die alle im **Konsens** verabschiedet wurden, belegen die Fähigkeit zur Einigung innerhalb der DSK.
Vorteil der föderalen Struktur: Landesbeauftragte sind näher am Unternehmen und am Betroffenen

Rechtsentwicklungen

Unklarheiten bei der Anwendung der DS-GVO sind europäisch angelegt,

Phase der Feinjustierung und Klarstellung dauert an:

- **Verwaltungsvorschriften**
  Der EDSA hat 16 „working papers“ aus der Zeit vor der DS-GVO übernommen, zwischenzeitlich 8 weitere „Guidelines“ (überwiegend noch in Konsultation), 11 „Expert Subgroups“ arbeiten an unzähligen weiteren Papieren
- **Rechtsprechung**
  obergerichtliche Entscheidungen stehen noch aus, Vorlagepflicht des nationalen (letztinstanzlichen) Gerichts gemäß Art. 267 Abs. 3 AEUV bei Fragen zum Unionsrecht, Verfahrensdauer EuGH ca. 17 Monate
- **Änderungsbedarfe der DS-GVO**
  Evaluierung der DS-GVO durch die DSK mit dem Ziel, den Prozess durch Stellungnahme zu unterstützen,
  Berichtsentwurf enthält Schwerpunkte (u.a. Informationspflichten, Recht auf Kopie, Datenpannenmeldungen, Meldung von Datenschutzbeauftragten, Zweckbindung) und macht konkrete Änderungsvorschläge - Übereinstimmung mit den Positionen der Wirtschaft

Missachtet die DS-GVO die neuen Geschäftsmodelle?

- **These**: DS-GVO missachtet die neuen Geschäftsmodelle:
  Big Data i. V. m. Künstlicher Intelligenz und Wirtschaft 4.0:
  - Wie passen Erfordernisse der Einwilligung, Datensparsamkeit, und Zweckbindung mit Wirtschaft 4.0/Big Data zusammen?
  - Datenschatz statt Datenschutz!
  - Neue „Datensouveränität“!
  - Maschine/Algorithmen und Mensch – Art. 22 DS-GVO

- **Gegenthese/Lösungen**: Datenschatz **mit** Datenschutz!
  - sachbezogene Informationen (Logistik) – aber: Informationssicherheit beachten
  - Eigentumsrecht an Daten? Ökonomisierung der Daten?

  - Ergänzend: Wettbewerbsrecht; Haftungsrecht
  - Verbindung von Recht und Technik in der Datenschutz-Folgenabschätzung gemäß DS-GVO
  - i. V. m. Data Protection by Design (Datenminimierung, Anonymisierung, Pseudonymisierung) (Marktchance) *Problem bei Anonymisierung: Re-Identifizierung!*
  - Künstliche Intelligenz (intelligente Privatsphäre-Assistenten; Verbraucher-Datenportale) (Marktchance)
  - Algorithmen: Transparenz, Kontrolle, Regulierung, Datenethikkommission
- **Verfassungsrechtlicher Einwand**: Verbot der zwangsweisen Registrierung des Menschen in seiner ganzen Persönlichkeit auch mittels anonymer Daten und Verbot der Totalüberwachung (Menschenwürde und Freiheit der Persönlichkeit)
- Vgl. Hambacher Erklärung der DSK zu KI von April 2019

Ausblick

- Europäische und nationale Gesetzgebung zur **Konkretisierung der DS-GVO** muss beobachtet werden, insbesondere
  - die ePrivacy-Verordnung
  - die weitere Entwicklung des speziellen Datenschutzes auf Bundes- und Landesebene

- Datenschutz ist komplexer, komplizierter und strenger geworden, daher:

- **Datenschutz bleibt Chefsache** - Verantwortlicher i. S. v. Art. 4 Nr. 7 ist die Stelle, die über Zwecke und Mittel der Datenverarbeitung entscheidet – vertreten durch die Leitung

Vielen Dank für Ihre Aufmerksamkeit!

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Geschäftsstelle und Besucheradresse: Leiterstraße 9, 39104 Magdeburg
Postadresse: Postfach 1947, 39009 Magdeburg
www.datenschutz.sachsen-anhalt.de
poststelle@lfd.sachsen-anhalt.de

Telefon: 0391 81803-0
Telefax: 0391 81803-33

SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz