Aktuelle Themen der Datenschutzaufsicht in Hessen

GI-Regionalgruppe Rhein-Main
27. April 2022

Prof. Dr. Alexander Roßnagel
Der Hessische Beauftragte für
Datenschutz und Informationsfreiheit
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Telefon: 0611 / 1408-0
Internet: https://datenschutz.hessen.de
E-Mail: poststelle@datenschutz.hessen.de

Übersicht

- Neue Aufgaben, neue Erfahrungen
- Aufgaben und Befugnisse der Datenschutzaufsicht
- Tätigkeitsbereiche der Datenschutzaufsicht
- Clouds, Videokonferenzsysteme und internationale Datentransfers
- Digitalisierung der Kommunikation und Gewährleistung der Vertraulichkeit
- Facebook-Fanpages
- Forschungsdaten: Datennutzung und Datenschutz
- Fazit & Ausblick

Neue Aufgaben und neue Erfahrungen

- Aufgaben eines Hochschullehrers
  - Interpretation und Systematisierung des Datenschutzrechts Vorschläge zur Fortentwicklung
  - Interdisziplinäre Forschungsprojekte zu künftigen IT-Anwendungen
  - Publikation von Forschungsergebnissen und Kommentaren zu Datenschutzgesetzen
  - Förderung des wissenschaftlichen Nachwuchses und Betreuung von Qualifikationsarbeiten

- Aufgaben des Leiters einer Datenschutzaufsichtsbehörde
  - Konfrontation mit der Praxis der Datenverarbeitung (Beschwerden, Dienstaufsichtsbeschwerden)
  - Notwendigkeit bindender Entscheidungen über praktische Datenschutzprobleme
  - Konfrontation mit den Folgen dieser Entscheidungen (Interessen, Widerstände)
  - Konfrontation mit Herausforderungen aus allen (digitalisierten) Lebenbereichen
  - Leitung einer selbständigen obersten Landesbehörde mit 55 Beschäftigten

Gesetzliche Aufgaben und Befugnisse der Datenschutzaufsicht

- 22 Aufgaben nach Art. 57 DSGVO und 18 Aufgaben nach § 13 ff. HDSIG
  - die Anwendung der DSGVO überwachen und durchsetzen
  - die Öffentlichkeit und die Verantwortlichen für die Risiken sensibilisieren und aufklären
  - sich mit Beschwerden einer betroffenen Person befassen
- 26 Befugnisse nach Art. 58 DSGVO und 9 Befugnisse nach § 14 HDSIG
  - Informationsanfragen, Datenschutzüberprüfungen, Hinweise, Zugangserzwingungen
  - Warnungen, Verwarnungen, Anweisungen, Beschränkung/Untersagung der Datenverarbeitung
  - Beratungen, Billigung von Verhaltensregeln, Akkreditierung von Zertifizierungsstellen
- Charakter der Datenschutzaufsicht
  - Strategische Zielauswahl und Schwerpunktsetzung (Regulierung statt Vollzug)
  - Regulatorische Durchsetzung (Planung, Ermessen statt gebundene Entscheidung)
  - Konstruktive Suche (gemeinsame nachhaltige Lösung statt einseitige Anordnung)

Tätigkeitsbereiche der Datenschutzaufsicht

- Fallbearbeitungen
  - Beschwerden (5.179), Beratungen (2.123), Verstoß-Meldungen (2.016), Geldbußen (29), Prüfungen, Anordnungen (32)
- Begleitungen, Interventionen
  - Infrastrukturen, Gesetzgebung (34), Projektkonzeptionen, Projektumsetzungen
- Initiativen
  - Beseitigung von Fehlentwicklungen, Reaktionen auf Urteile, Nachregulierung nach Corona
- Hessische, nationale und internationale Zusammenarbeit
  - Ausschuss für Digitales und Datenschutz, E-Government-Rat, AK Sicherheit
  - DSK und viele AKs, UAKs und Task Forces, Adhoc-AGs, gemeinsame Fallbearbeitungen
  - EDSA und viele Subgroups, Amtshilfe, europäische Kooperation (IMI) (1.074)

Internationaler Datenverkehr

- EuGH (Schrems II vom 16.7.2020): Grundrechtsverlust verhindern
  - Unverhältnismäßige Befugnisse (FIS-Act) (gilt auch für CLOUD-Act)
  - Fehlender Rechtsschutz für US-Ausländer
- Rechtsfolge
  - Prüfpflicht der Verantwortlichen, ob in Drittstaat angemessenes Schutzniveau herrscht (für USA durch EuGH festgestellt: nein)
  - Datenübermittlung nur zulässig, wenn zusätzliche technisch-organisatorische Schutzmaßnahmen Zugriff verhindern
- Digitale Selbstbehauptung fordert digitale Souveränität
  - Verantwortlicher nutzt IT, die datenschutzrechtliche Vorgaben einhält
- EuGH: Aufsichtsbehörde hat dies durchzusetzen

Corona und Videokonferenzsysteme

- Notwendigkeit des Nachjustierens
  - Nutzung datenschutzrechtskonformer Videokonferenzsysteme
- Ausübung pflichtgemäßen Vollzugsermessens
  - Berücksichtigung von Aufgaben und Grundrechten
  - Suche nach geeigneten Alternativen
- Handlungsmöglichkeiten der Verantwortlichen
  - Auswahl der Anbieter (ohne Verpflichtung gegenüber US-Recht)
  - Eigenbetrieb der IT-Systeme
  - Privacy by Design: Architektur der Videokonferenzsysteme, Informationssicherheit und Gewährleistung der Datenschutzgrundsätze
  - Privacy by Default: Datenschutzgerechte Konfiguration der Systeme und Vorgaben an ihre Nutzung

Digitalisierung und Gewährleistung von Vertraulichkeit

- Vorteile der Digitalisierung der Kommunikation
  - Möglichkeit sicherer Authentifizierung
  - Möglichkeit sicherer Verschlüsselung
  - Möglichkeiten des sicheren Up- und Downloads von Daten

- Defizite der Fax-Kommunikation
  - Paketartige Übermittlung über IP-Netze statt exklusive Verbindung zweier Anschlüsse
  - Unsicherheit über Empfänger (Umwandlung in Mail/Speicherung auf Mailserver)
  - Mangelnde Identifizierung des Empfängers
  - Kein Vertraulichkeitsschutz wegen fehlender Verschlüsselung

Datenschutzgemäße Lösungen

- Hinweis auf datenschutzrechtliche und berufsrechtliche Verpflichtungen
  - Orientierung am Stand der Technik – Schutz der anvertrauten Grundrechte
  - Keine Geschäfts- und Verwaltungsmodelle auf der Grundlage von Einwilligungen möglich
  - Umstieg auf alternative Kommunikationsmittel notwendig
  - Zeit für notwendigen Transformationsprozess

- Mögliche Alternativen durch digitale Kommunikation
  - Verschlüsselte E-Mail (PGP oder S/MIME), DE-Mail
  - Berufs- oder bereichsspezifische Lösungen (EGVP/beA/beN/beBPo, KIM, …)
  - Portallösungen (verschlüsselte Upload- und Downloadmöglichkeiten)
  - ekom21: Elektronischer sicherer Nachrichtenaustausch (esina21)
  - Bürgerpostfach nach OZG

Rechtswidrige Datenverarbeitung bei Facebook Fanpages

- Abschluss eines zehnjährigen Gerichtsprozesses
  - EuGH 2018: Gemeinsame Verantwortung von Seitenbetreiber und Facebook
  - OVG Schleswig-Holstein 25.11.2021: „schwerwiegender datenschutzrechtlicher Verstoß“
- Rechtswidrige Datenverarbeitung durch Facebook (Profilbildung) – Mitverantwortung des Seitenbetreibers
  - Keine Vereinbarung zur gemeinsamen Verantwortung gemäß Art. 26 DSGVO
  - Keine ausreichende Information über Datenverarbeitung nach Art. 13 DSGVO
  - Keine Einwilligung in Cookie-Nutzung – Verstoß gegen § 25 TDDSG
  - Keine ausreichenden Schutzmaßnahmen bei Datentransfer und Datenverarbeitung gegen Zugriff von US-Behörden (Schrems II-Problem)

Datenschutzrechtliche Folgen

- Gemeinsame Bewertung und Absprache der Datenschutzaufsichtsbehörden
  - DSK-Taskforce: Überprüfung der neuesten Datenverarbeitung und des OVG-Urteils
  - Beschluss der DSK vom 23.3.2022: Datenverarbeitung rechtswidrig und zu unterlassen
  - Information der öffentlichen Stellen durch die meisten Aufsichtsbehörden (ab 7.3.2022)
- Datenschutzrechtliche Situation
  - Feststellung der Rechtswidrigkeit: Beschwerden, Schadensersatz, Fragen der Opposition
  - Verfassungsrechtlicher Auftrag der Öffentlichkeitsarbeit (Problem der Reichweiten)
  - Handlungsmöglichkeiten: Druck auf Facebook oder Wechsel des Netzwerks
  - Koordination aller öffentlichen Stellen erforderlich
  - Transformation benötigt Zeit (Aufbau von Alternativen), die zu gewähren ist
  - Einfordern der Deaktivierung von Facebook-Seiten

Forschungsdaten: Datennutzung und Datenschutz

- Schwerpunkt der DSK 2022: Nutzung der Forschungsdaten mit Datenschutz
- Forschung ist Grundrecht (Art. 13 GRCh) und Allgemeininteresse
  - Bevorzugung in der DSGVO: Art. 5 I b und e, 9 II j, „broad consent“
  - Ausgleich durch geeignete Garantien: Anonymisierung, Pseudonymisierung, Datensparsamkeit
- Neue Regelungen: Data Governace Act und Data Act
  - Öffentliche Stellen: Open Data mit Schutz gegen Personenbezug: z.B. Anonymisierung
  - Datenmittler im Datenmarkt: gesonderte Rechtsperson ohne eigene Absicht der Datenverarbeitung, Registrierung möglich, Unterstützung betroffener Personen
  - Datenaltruistische Organisationen: akkreditiert, unabhängig von Erwerbsorganisationen und ohne Erwerbszweck, Verwaltung von Datenspenden, Sicherung der Zweckbindung
  - Nutzung der Daten: Schutz vor missbräuchlichen Vertragsklauseln, Zugang der Nutzer vernetzter Produkte (IoT) zu den Daten, Datenübertragung zur Erleichterung des Wechsels

Datenschutzrechtliche Probleme

- Anwendbarkeit von Datenschutzrecht
  - Keine eigenständigen Regelungen in DGA und DA zum Datenschutz („bleibt unberührt“)
  - Verweis auf abstrakte Regelungen der DSGVO
- Einwilligung
  - Informiert? Zwecke und Empfänger, Dauer der Speicherung
  - Bestimmt? Stellvertretung? Sicherstellung der Zweckbindung? Widerruf und Folgen?
- Datenübertragung
  - DSGVO: Nur pD, die von betroffener Person bereitgestellt wurden, Einwilligung oder Vertrag
  - DA: alle Daten, Verhältnis weitergabeberechtigter Nutzer und betroffene Person?
- Anonymisierung
  - DSGVO, DGA, DA: Keine Definition und keine Regelung – Aufgabe öffentlicher Stellen und Datentreuhänder

Fazit & Ausblick

- Der HBDI ist keine normale Behörde
  - Er ist unabhängige oberste Landebehörde mit Generalauftrag zur strategischen Regulierung
- Er hat ein extrem breites Tätigkeitsfeld
  - Er muss in allen Bereichen und auf allen Ebenen der Gesellschaft für Grundrechte eintreten
- Er ist eingebunden in das Netz der Aufsichtsbehörden
  - Nationale und internationale Kooperationen sorgen für einheitlichen Datenschutz
- Er bearbeitet wichtige Themen für die digitale Gesellschaft
  - Gewährleistung von Datenschutz ist ein Grundpfeiler einer lebenswerten Zukunft