Dies ist einen Zusammenfassung des Vortrags „Jahresrückblick 2024“ von Kirsten Bock in der Dezember-Ausgabe der Reihe „Datenschutz am Mittag“.
URL: **https://sds-links.de/DSaM_12-2024**

Datenschutz verstehen wir als Grundrecht auf Freiheit von Überwachung, aber auch auf das Recht auf analogen Zugang zum gesellschaftlichen Leben. Zahlreiche Entwicklungen , wie die weiter zunehmende Digitalisierung, anstehenden Verschärfungen im Asylrecht, die neuen Sicherheitsgesetze oder die Vorschläge der „Going Dark-Gruppe“ machen es notwendig, über einen datenschutzrechtlichen Anspruch auf die Freiheit von Überwachung nachzudenken.

Aus den Aufsichtsbehörden:

- In Sachsen-Anhalt (Maria Christina Rost) und in Thüringen (Tino Melzer) wurden neue Landesbeauftragte für den Datenschutz gewählt (Datenschutz am Mittag zum Berufungsverfahren von Landesbeauftragten)
- als Bundesbeauftragte trat Louisa Specht-Riemenschneider die Nachfolge von Ulrich Kelber an.
- auch 2024 haben Aufsichtsbehörden zahlreiche Stellungnahmen und Handreichungen zur praktischen Anwendung des Datenschutzrechts veröffentlicht. Die Zusammenarbeit im Rahmen der Datenschutzkonferenz konnte nicht grundlegend verbessert werden.
- Spitzenreiter bei den in der EU verhängten Bußgeldern war die irische Data Protection Commission mit einem 310-Millionen-Euro-Bußgeld gegen LinkedIn. Dem Unternehmen wird vorgeworfen, personenbezogene Daten unrechtmäßig für Verhaltensanalysen und gezielte Werbung zu nutzen. Das Verfahren war 2018 von der französischen Bürgerrechtsorganisation „La Quadrature du Net“ initiiert worden. Bei der Höhe der insgesamt verhängten Bußgelder wird wohl wieder die CNIL das Ranking anführen.

EDSA Leitlinien

- 1/2024 Berechtigtes Interesse (vorläufige Version) https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en
- 2/2024 Art. 48 Übermittlung von Daten aufgrund Urteils oder Anordnung einer Behörde in einem Drittland (Konsultation läuft) https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-022024-article-48-gdpr_en
- 2/2023 zum technischen Anwendungsbereich des Art. 5.3 ePrivacy, final
- Und eine Opinion zu KI https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_en
- 28/2024 Auffassung zu ausgewählten Aspekten mit Bezug zur Verarbeitung beim Training von KI-Modellen https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

EU Kommission

Zweite Evaluation der DSGVO: Rückmeldungen generell positiv, nur aus DE eher negativ
EU-Kommission fordert effizientere Zusammenarbeit der Datenschutzbehörden auf nationaler und europäischer Ebene,

Bundesrat:
Forderung nach DSGVO-Reform, Ergebnis: Keine Novelle

EU Digitalstrategie: Europe fit for Digital Age
Digital Services Act: seit 17. Februar 2024 anwendbar

KI-Verordnung: EU-Parlament stimmt für KI-VO, am 12. Juli 2024 im Amtsblatt der Europäischen Union veröffentlicht; Geltungsbeginn 2. August 2026, allerdings mit Ausnahmen. Ab dem 2. Februar 2025 gelten zunächst Verbote für bestimmte KI-Praktiken, wie biometrische Echtzeit-Fernüberwachung und Social Scoring. Mitgliedsstaaten müssen bis zum 2. August 2025 Durchführungsvorschriften erlassen, in denen die Behörden benannt werden, die für die Durchsetzung der KI-Verordnung zuständig sind.

Künstliche Intelligenz
Mit Inkrafttreten der KI-Verordnung stellen sich nicht nur ethische und praktische Fragen im Umgang mit Anwendungen künstlicher Intelligenz, sondern nun auch die Frage nach dem Verhältnis von Datenschutz und KI. Dazu sind bereits zahlreiche Leitfäden, Checklisten und Arbeitspapiere erschienen.

- **Januar: Datenschutz am Mittag: Kann die DSGVO Künstliche Intelligenz sinnvoll regulieren?** Webinar mit Dr. Sabine Schäufler; BayLDA: „Datenschutzkonforme Künstliche Intelligenz" – Checkliste mit Prüfkriterien; Prüfverfahren der italienischen Aufsichtsbehörde bei ChatGPT stellt mehrere Verstöße gegen die DSGVO fest.
- **März:** LfDI NRW weist zur Verabschiedung der KI-Verordnung darauf hin, dass oft schwer festzustellen ist, ob personenbezogene Daten in KI-Systemen verarbeitet werden.
- **April**: EDSA bildet Taskforce zu ChatGPT. Ein Arbeitsbericht befasst sich mit einzelnen Phasen der Verarbeitung: Erhebung der Trainingsdaten, Vorverarbeitung, Training, Nutzereingaben/Prompts, Ausgaben und Training durch Prompts. Demnach sind die Erhebung und Vorverarbeitung sowie das Training selbst besonders kritisch, weil die Daten durch Scraping im Web automatisiert erhoben werden; Art. 6 Abs. 1 lit f ist keine geeignete Rechtsgrundlage; die Einhaltung der Grundsätze aus Art. 5 (Fairness, Transparenz, Richtigkeit) ist fraglich. Zur Frage KI Training unter Art. 6 Abs. 1 lit f ist eine Leitlinie angekündigt, weil die Probleme nicht erst bei der Nutzung, sondern schon beim Training von KI-Anwendungen entstehen.
- **Mai:** Die Datenschutzkonferenz (DSK) veröffentlicht eine Orientierungshilfe mit datenschutzrechtlichen Kriterien für die Auswahl und den Einsatz von KI-Systemen. Schwerpunkte sind Auswahl und Einsatz von Large Language Models (LLM) und Chatbots Die DSK rät in Zweifelsfällen, eine DSFA zu erstellen.
- **Juni:** Die französische Aufsichtsbehörde CNIL gibt Empfehlungen zur Entwicklung von Systemen der künstlichen Intelligenz und bezieht sich im Kern auf die klassische Anwendung der DSGVO:
  - das anwendbare Rechtssystem bestimmen;
  - einen Zweck definieren;
  - die rechtliche Einstufung der Akteure bestimmen;
  - eine Rechtsgrundlage definieren;
  - Tests und Prüfungen im Falle einer Weiterverwendung der Daten durchführen;
  - gegebenenfalls eine Folgenabschätzung durchführen;
  - den Datenschutz bei der Gestaltung des Systems berücksichtigen;
  - den Datenschutz bei der Erhebung und Verwaltung von Daten berücksichtigen.

Ergebnis: Für definierte, zweckgebundene Einsatzbereiche können ethisch vertretbare Anwendungen entwickelt werden.
Die irische Aufsichtsbehörde DPC erklärt das KI-Training mit Meta-Nutzerdaten (Facebook, Instagram, Threads) für unzulässig; Art. 6 Abs. 1 lit f kann nicht Rechtgrundlage sein.
Der EDSA stellt am 27. Juli einen KI- Auditing Katalog mit Anforderungen an Tools vor, die helfen sollen, die Rechtskonformität von KI-Systemen und Anwendungen zu prüfen.

- **Juli**: Der Hamburger LfDI: *„Die bloße Speicherung eines LLMs stellt keine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar und mangels Speicherung von pbD sei auch die DSGVO nicht anwendbar. Zwar würde das Training mit pbD unter die DSGVO fallen, allerdings würde sich ein rechtswidriges Training nicht auf die Rechtmäßigkeit des Einsatzes auswirken.“*
  Diese Auffassung dürfte als abweichende Ansicht in die Annalen eingehen. Notwendig ist besseres Verständnis der Technik und des Verarbeitungsbegriffs.
- **August:** Die BayLDA erweitert ihr Informationsangebot zu KI und Datenschutz um einen Themenschwerpunkt und wirbt dafür, die Aufsicht über die KI-VO bei der Datenschutzaufsicht zu belassen und nicht zu zentralisieren.
- **November:** EDSA Stakeholder Veranstaltung zu KI-Modellen
- **Dezember**: EDSA Stellungnahme 28/2024 zu bestimmten Datenschutzaspekten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen von KI-Modellen

Zivilgesellschaft und KI
Die Gruppe D 64 veröffentlicht ein White Paper über den Freiheitsbegriff im Kontext von KI zu einem Code of Conduct Demokratische KI.

- verengt Argumentation auf „Transparenz, Einwilligung und Kontrolle“
- Kontrolle muss sich auf alle grundrechtsrelevanten Aspekte beziehen
- Transparenz allein ist unzureichend
- Datenschutz ist notwendige Bedingung für Freiheit, weil Datenschutzrecht Kontrolle grundrechtsverträglich gestaltet
- Schutzziele des Datenschutz: Transparenz, Intervenierbarkeit, Bedingungen für Verknüpfung von Informationen (Nichtverkettung), Vertraulichkeit, Integrität und Verfügbarkeit

Die neueste Version des **Standarddatenschutzmodells** SDM 3.1 wurde am 14.5.24 von der DSK bestätigt. Alle DSK-Infos zum SDM beim LfD MV.

Einladung zur Mitarbeit in der **SDM User Group**! Tipp: Nicht in der Methodik „verheddern“, Schutzziele anwenden, und zwar auf allen drei Ebenen Daten, Systeme, Prozesse und in allen Phasen der Verarbeitung

(Un-)Sicherheitspaket der Bundesregierung: Gesichtserkennung im Fokus
Als Reaktion auf den tödlichen Angriff beim Stadtfest in Solingen im August schnürt die Bundesregierung im Oktober ein „Sicherheitspaket“. Biometrische Gesichtserkennung aus öffentlich zugänglichen Internetdaten soll ermöglicht werden. Der Gesetzentwurf hätte dem Bundesamt für Migration und Flüchtlinge (BAMF) erstmals erlaubt, Personen mittels automatisierter Stimm- und Gesichtserkennung zu überwachen und dafür Daten aus dem Internet zu nutzen. Bundeskriminalamt und Bundespolizei sollten Big-Data-Analysen mithilfe von KI durchführen.

CCC, FIfF und andere zivilgesellschaftliche Akteure warnen vor einem "biometrischen Überwachungsexzess". Die Ampel verfalle in blinden Aktionismus und wolle Anonymität faktisch beenden. Bündnis Gesichtserkennung stoppen
Einigen Ländern ging der Entwurf nicht weit genug. Der **Bundesrat** hat Teile des umstrittenen „Sicherheitspakets“ abgelehnt.

Rechtsprechung

Scraping und Immaterieller Schadenersatz, Art. 82 DSGVO

(Scraping: automatisiertes Abgreifen von öffentlich zugänglichen Website-Inhalten Beispiel: Meta-Scraping Fälle)
Gerichte landesweit befasst, zahlreiche Verfahren, uneinheitliche Rechtsprechung
Kein Anspruch auf **immateriellen Schadenersatz,** wenn der Schaden nicht konkret nachgewiesen wird (Beispiele: „Kontrollverlust“, „emotionales Ungemach“ und „Genervte Stimmung“ als Leerformeln zur Darlegung nicht ausreichend)
ABER: OLG Oldenburg hielt Sorgen für ausrechend, Urteile vom 30.04.2024: Ein Kläger war infolge des Scrapings in Sorge wegen eines möglichen Missbrauchs der Mobilfunknummer. Ihm wurde ein immaterieller Schaden im Sinne des Art. 82 Abs. 1 DSGVO zuerkannt. Ein anderer hatte durch den Scraping-Vorfall hervorgerufenen Ängste und Sorgen zusätzlich dadurch belegt, dass er sich eine zweite Mobilfunknummer zugelegt hat. Ihm wurde ein Schmerzensgeld i.H.v. 250 € zugesprochen.
Im November dann das **Leitentscheidungsverfahren beim BGH:** *„Auch der bloße und kurzzeitige Verlust der Kontrolle über eigene personenbezogene Daten infolge eines Verstoßes gegen die Datenschutz-Grundverordnung kann ein immaterieller Schaden im Sinne der Norm sein“*.
Missbräuchliche Verwendung von personenbezogenen Daten oder sonstige spürbare negative Folgen müssen nicht eingetreten sein.
Ergebnis: Bislang hatten die Gerichte Schadensersatzforderungen regelmäßig zurückgewiesen, wenn bloße Befürchtungen oder Ärgernisse ohne nachweisbare konkrete negative Folgen dargelegt wurden. In seiner Leitentscheidung stellt der BGH klar, dass keine besondere Beeinträchtigung durch die Betroffenen nachgewiesen werden muss. Der BGH hält einen Betrag von etwa 100 Euro als Schadensersatz für angemessen.
Im Dezember reicht der Verbraucherzentralen Bundesverband (VZBV) eine Musterfeststellungsklage gegen Meta ein. Diese hemmt drohende Verjährung von Schadenersatzansprüchen zum Jahreswechsel. Betroffene können sich dem Sammelklageverfahren voraussichtlich ab Anfang 2025 anschließen, wenn das Bundesamt für Justiz das Klageregister öffnet.

Weitere Verfahren zum Schadensersatz nach Art. 82 DSGVO

EuGH in MediaMarkt Saturn zur Frage, ob und unter welchen Umständen eine Person, Anspruch auf Schadensersatz hat, wenn deren Daten unrechtmäßig an Dritte weitergegeben wurden: Betroffene muss nicht nur Verstoß gegen die DSGVO nachweisen, sondern auch den ihr entstandenen **materiellen oder immaterieller Schaden**. Rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten, zB wenn kein Dritter die fraglichen personenbezogenen Daten zur Kenntnis genommen hat, unzureichend.

EuGH in Urteil vom 20.06.2024 (C-590/22) Sachverhalt: Steuererklärung, war ohne Einwilligung der Betroffenen an Dritte weitergegeben worden: Nicht jeder Verstoß gegen die DSGVO begründet einen Schadensersatzanspruch. Wortlaut der DSGVO unterscheide deutlich zwischen „Verstoß“ und „Schaden“, Schadensnachweis daher erforderlich. Einen bestimmten Schweregrad müsse der Schaden jedoch nicht erreichen. Selbst ein kurzzeitiger Kontrollverlust

reiche aus, auch wenn nicht nachgewiesen werden könne, dass die Daten tatsächlich an Dritte gelangt waren.

Verweis auf das „Volkszählungsurteil“ des BVerfG: „Ungutes Gefühl“ reicht

EuGH, Urteil vom 11.04.2024, Rs. C-741/21 (Volltext): Für eine Haftungsbefreiung nach Art. 82 Abs. 3 DSGVO ist es nicht ausreichend, dass der Datenschutzverstoß durch ein Fehlverhalten eines Beschäftigten verursacht wurde. Die Entscheidung ist auch in einem anderen Kontext interessant, dem sogenannten “Mitarbeiter-Exzess“. Der EuGH stellt hohe Hürden für Exkulpation des Unternehmens auf. Ein bloßer Verweis darauf, dass ein Mitarbeiter weisungswidrig gehandelt habe, reiche nicht aus, um die Haftung auszuschließen. Vielmehr müsse der Verantwortliche nachweisen, dass es keinen Kausalzusammenhang zwischen einem eigenen Verstoß gegen die DSGVO und dem Handeln des Mitarbeiters gibt. Mit dem alleinigen Verweis auf eine Datenschutzrichtlinie können sich Unternehmen vor dem Hintergrund dieser Argumentation künftig nur schwer gegen Schadensersatzansprüche verteidigen. Dies sollte von den Aufsichtsbehörden zukünftig berücksichtigt werden.

Die Rolle der Datenschutzbeauftragten

Der EDSA veröffentlichte im Januar die Ergebnisse der koordinierte Durchsetzungsmaßnahme zur Rolle von Datenschutzbeauftragten in den einzelnen Mitgliedstaaten. Kritik:

- Ressourcenausstattung genügt nicht den Anforderungen aus Art. 38 Abs. 2 DSGVO;
- Betrauung mit sachfremden Aufgaben schränkt angemessene Aufgabenerfüllung ein;
- Interessenkonflikte, wenn Datenschutzbeauftragte beispielsweise Managementaufgaben wahrnehmen oder externe Datenschutzbeauftragte sowohl den Verantwortlichen als auch den Auftragsverarbeiter vertreten.

Bayerisches LDA hat einen 16-seitigen Prüfbogen veröffentlicht zur Qualifikation und Ressourcenausstattung. Ergebnisse zu der Untersuchung sind noch nicht veröffentlicht.
Hinweis: **DPOCert** ermöglicht standardisierten Nachweis der Qualifikation durch DAkkS-Akkreditierung.

DSGVO und Recht der Kirchen noch nicht harmonisiert

Belgische Datenschutzaufsichtsbehörde hat in einem Beschwerdeverfahren entschieden, dass die lebenslange Verarbeitung von personenbezogenen Daten einer Person, die ihren Austritt aus der **römisch-katholischen Kirche** beantragt hat, aus datenschutzrechtlicher Sicht nicht zu rechtfertigen ist. Die Behörde hat die Diözese Gent daher angewiesen, die Daten des Beschwerdeführers zu **löschen**.
Dagegen im März veröffentlicht: LAG Baden-Württemberg, Urteil vom 27.10.2023, Az. 7 Sa 35/23 (juris): Im Lichte der Kirchenklausel in Art. 17 Abs. 1 AEUV i.V.m. Art. 91 Abs. 1 DSGVO sind die kirchenrechtlichen Datenschutzregelungen grundsätzlich vorrangig anwendbar und verdrängen die DSGVO.

Gesundheitsdaten:

DSK-Stellungnahme zum Teilen von Gesundheitsdaten mit Krankenkassen und Freigabe zur Drittnutzung, insbesondere zu den Anforderungen an die Sekundärnutzung genetischer Daten zu Forschungszwecken. DSK fordert weitere gesetzliche Regelungen. Einschätzung: Einwilligungslösung wäre unzureichend; erforderlich sind substantielle Anforderungen an die Verarbeitung, insbesondere auch die Systeme. Problem: Untersuchung und Forschung/Übermittlung in die USA.

Gesundheitsminister Karl Lauterbach: Daten in der elektronischen Patientenakte sind „Goldgrube“ für Pharmaunternehmen. Ziel: Daten aus der ePA effektiver nutzen und Daten aus den ePA Unternehmen wie Google und Meta zur Verfügung stellen, um Künstliche Intelligenzen damit trainieren zu können. Außerdem sollen Patientinnen und Patienten die Daten aus der elektronischen Patientenakte als „Datenspende“ dem Bundesinstitut für Arzneimittel und Medizinprodukte zur Verfügung stellen.
Einschätzung: Unkenntnis der Entscheidungen des EuGH, der Grundrechte und Risiken erschweren sachgerechte Diskussion und Entscheidungen in der Politik.

Das rosa Papier-Rezept wurde durch E-Rezept abgelöst und ist für gesetzlich Versicherte bei verschreibungspflichtigen Arzneimittel obligatorisch. E-Rezepte können per elektronischer Gesundheitskarte (eGK), Papierausdruck oder per E-Rezept-App (Gematik-App oder App der Krankenkassen) eingelöst werden; dies ist eine Pflichtanwendung des deutschen Gesundheitsnetzes, der Telematikinfrastruktur (TI). Rezepte werden nicht auf der elektronischen Gesundheitskarte (eGK) gespeichert. Zugriffsmöglichkeiten: E-Rezept-App, Lesegerät für die eGK durch Apotheke (Zugriff unterschiedslos auf alle Rezepte), 2D-Code Ausdruck auf Papier durch die Arztpraxis.

TikTok

- Politiker:innen legen TikTok-Accounts an
- Wahlbeeinflussung – was hat das mit Datenschutz zu tun?
- Profiling durch Algorithmen
- LfDI Baden-Württemberg veröffentlicht Checkliste mit Fragen zu TikTok
- Datenschutzkonformer Einsatzes durch Behörden und andere öffentliche Stellen? Allein mit Kontoeinstellungen ist es nicht getan, Alternativkanäle auf die Bürger:innen sicher und unbeobachtet zugreifen können, sind eine gute Option.

Stand der Vorhaben der Bundesregierung

Beschäftigtendatenschutz

Kein Entwurf schaffte es über die Ressortabstimmung hinaus.
LAG Düsseldorf, Urteil vom 10.04.2024, Az. 12 Sa 1007/23: Arbeitgeber muss über Google-Recherche gemäß Art. 14 DSGVO informieren und Datenkategorien (Art. 14 Abs. 1 lit. d DSGVO) präzise und spezifisch benennen, damit Betroffene die Risiken abschätzen kann.

„**Digitalcheck Datenschutz**“:

Regelungsvorhaben mit Digitalbezug sollen erfasst werden und Gewährleistung von Datenschutz und Datensicherheit unterstützen. Einschätzung: Geht bislang über Erfassung nicht hinaus.

Überwachungsgesamtrechnung

Bundesministerium der Justiz vergibt im Januar 2024 Auftrag zur wissenschaftlichen Untersuchung der Sicherheitsgesetze an Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht. Noch bevor die Ergebnisse vorliegen: Innenminister:innen der Länder lehnen Überwachungsgesamtrechnungsvorhaben ab

Einsatz von Microsoft 365

Im März stellt der **EDSB** fest , dass die EU-Kommission beim Einsatz von Microsoft 365 gegen datenschutzrechtliche Vorgaben verstößt:

- Kategorien personenbezogener Daten nicht hinreichend bestimmt
- Zwecke nicht definiert
- keine angemessene Garantien bei Drittlandsübermittlungen
- unklare Regelung zur Weitergabe von Daten

Im Mai erhebt die EU-Kommission beim EuGH Klage gegen den EDPS; vier Tage später klagt auch Microsoft.

Niedersachsens LfDI billigt Einsatz von MS Teams

Das Land Niedersachsen hat einen Vertrag mit Microsoft über den Einsatz von Microsoft Teams abgeschlossen, der die Bedenken der deutschen Datenschutzaufsichtsbehörden ausräumen soll. Pressemitteilung vom 26. April 2024?

Dieser könnte als Blaupause für den Einsatz von Microsoft 365 durch öffentliche Stellen in Deutschland dienen. Voraussetzung für die Datenschutzkonformität bleibt eine Datenschutz-Folgenabschätzung. Einschätzung: Die Rolle des LfDI beschränkt sich auf die Bewertung des Verhandlungsergebnisses. Demnach ist die Ausgestaltung des Auftragsverarbeitungsvertrages akzeptabel. Offen bleibt die Frage, ob auch die Datenverarbeitungen selbst den Anforderungen der DSGVO entsprechen, die der LfDI zwar formuliert, deren Einhaltung aber wohl nicht geprüft wurde.

Blick über die Grenze

Spanien

Die spanische Datenschutzaufsichtsbehörde richtet eine Innovationsabteilung ein, die sich mit neuen Technologien befasst

EU-U.S. Data Privacy Framework (DPF)

Beschwerdeformular abrufbar bei BfDI. Einschätzung: Wirksamkeit des Beschwerdewegs bleibt fraglich.

EDSA

Erster Bericht über die erste Überprüfung des EU-U.S.-Datenschutzrahmens: Zahl der Beschwerden gering. EDSA hält es für notwendig, dass die US-Behörden Überwachungsmaßnahmen einführen, um zu überprüfen, ob zertifizierte US-Unternehmen die wesentlichen Grundsätze des DPF tatsächlich einhalten. Einschätzung: Die Wiederwahl von Donald Trump wird es erforderlich machen, die Einhaltung des Frameworks sorgfältig zu beobachten, um frühzeitig eingreifen zu können.

Chatkontrolle

Der Versucht, eine anlasslose Massenüberwachung einzuführen, steht weiterhin in der Kritik, auch beim im September ausgeschiedene BfDI Ulrich Kelber: „Die Durchleuchtung sämtlicher privater Nachrichteninhalte ist keine Option. Der Verordnungsentwurf der Kommission in seiner ursprünglichen Form darf daher nicht realisiert werden...“. Österreich befürwortet die Aufhebung der Messenger-Verschlüsselung und fordert Zugriff auf Kommunikation der EU-Bürger. Ende Juni scheitern die Verhandlungen über die sogenannte Chatkontrolle zwischen den EU-Staaten vorerst.

Cybersicherheit
Ein Angriff mit Ransomware offenbart nicht zwingend Datenschutzverstöße. Die Zahl der Angriffe nimmt weiter zu. Einschätzung: Gutes Datenschutzmanagement hilft

Zertifizierung
Die Aufsichtsbehörde Nordrhein-Westfalen erteilt erstmals in Deutschland die Befugnis, Datenverarbeitungsprozesse zu zertifizieren. Akkreditiert wird die **EuroPriSe Cert GmbH** am 2.2.2024. Auftragsverarbeiter können Datenverarbeitungsprozesse gemäß DSGVO von EuroPriSe Zertifikat „European Privacy Seal" (EuroPriSe) auszeichnen lassen. Einschätzung: Zertifikate sind ein bewährtes Instrument zur Marktorientierung und Einhaltung der Grundsätze der DSGVO und schaffen Überblick über das Datenschutzniveau.
Der Bundesrat forderte kürzlich verpflichtende Zertifizierung von Produkten und IT-Dienstleistungen auf ihre DSGVO-Konformität. DSGVO regelt Zertifizierung von Datenverarbeitungen, nicht direkt für Hersteller von „Produkten".
Einschätzung: Produkte werden idR als „Service" angeboten. Insofern sind Hersteller bereits gefordert; Produkte und Dienstleistungen für konkrete Zwecke rechtskonform eingesetzt werden können. Auch bei dieser Frage zeigt sich, dass mehr Fortbildung und Sachwissen im Datenschutzrecht für politische Entscheidungsträger:innen hilfreich ist.

Recht auf analoges Leben?
Das politische Frühjahrsforum des BfDI stand unter dem Motto "Ausschließlich digital? – Wie weit geht das Recht auf ein analoges Leben?" Leider gibt es davon keine Aufzeichnung. Auch der Europäische Datenschutztag am 28.01.2025 in der Hessischen Landesvertretung hat „Digitalisierung um jeden Preis? Kein Zwang zur Preisgabe personenbezogener Daten" zum Thema

Schlaglichter (im Vortrag nicht behandelt)
- LfD Thüringen: Telefax ist kein sicheres Transportmittel „FAX: kein Klacks!" Es kommt für die datenschutzrechtliche Beurteilung allerdings immer auf die Umstände des Einzelfalls an.
- LG Hamburg, Urteil vom 22.02.2024, Az. 327 O 250/22: Für eine Bestellung auf einem Online-Handelsmarktplatz kann die Anlage eines fortlaufenden Kundenkontos verlangt werden.
- EDSA: Europaweite Kontrollaktion (Fragebogen) zum Recht auf Auskunft.
- LG Berlin: Abschöpfung von Daten (Hacker-Angriff) durch Dritte ist keine Verarbeitung des Verantwortlichen. Informationen über einen Datenschutzvorfall unterfallen nicht dem Auskunftsrecht, Art. 15 DSGVO.
- CNIL kritisiert, dass die meisten Studien zur DSGVO sich lediglich mit den wirtschaftlichen Auswirkungen/Kosten befassen, ohne den Nutzen für die Unternehmen und die Gesellschaft ausreichend zu messen.
- EuGH, in IAB Europe: Transparency-and-Consent-String ist ein personenbezogenes Datum, wenn er mit vertretbarem Aufwand einer natürlichen Person zugeordnet werden kann.
- EDSA: Consent or Pay-Modelle sollen echte Wahlmöglichkeiten i.S. einer gleichwertigen Alternative schaffen. Personenbezogene Daten können nicht als handelbare Ware betrachtet werden und dass das Grundrecht auf Datenschutz darf nicht kostenpflichtig werden. Die DSK hatte im Mai 2023 sog. Pur-Abo Modelle gebilligt. Einschätzung: Die Entscheidungen widersprechen sich. Nach Meinung des EDSA wird es in den meisten Fällen nicht

möglich sein, die Anforderungen an eine wirksame Einwilligung zu erfüllen, wenn den Nutzenden vor die Wahl zwischen der Einwilligung in die Verarbeitung personenbezogener Daten für verhaltensbezogene Werbezwecke und der Zahlung einer Gebühr gestellt wird.

- HBDI: „Parkraumüberwachung durch Parkvision nach Einschreiten des HBDI an DS-GVO angepasst“: Funktionsweise des Überwachungssystems nicht nachvollziehbar und nach Androhung einer Untersagung hat Parkvision sein System offenbar verändert.
- Einschätzung: Leider keine konkreteren Hinweise durch den hessischen Beauftragten.
- Kontext: Überwachungsgesamtrechnung, System ermöglicht Erstellung weitreichender Bewegungsprofile.
- EuGH in Meta vs. VZBV: Voraussetzungen für Verbandsklagen präzisiert. Bundesregierung: Cookie-Einwilligungsverwaltungsverordnung, § 26 Absatz 2 TDDDG. Einschätzung: „Man in the Middle“ soll Nutzer:innen helfen, Einwilligungen zu verwalten. Kein echter Gewinn; sinnvoller wäre eine Regelung zum Einsatz von Cookies (Speicherumfang, Lebensdauer).
- DSK Positionspapier zu den Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG): Bezahlkarte greift in das Recht auf informationelle Selbstbestimmung und die Datenschutzgrundrechte aus der EU-Grundrechtecharta ein. Einschätzung: Aufweichungen des DSGrundrechts werden im Bereich Ausländerzentralregister und Asylbewerber geprobt, dort ist am wenigsten Widerstand zu erwarten und es tritt ein Gewöhnungseffekt ein
- Bundesverfassungsgericht: Teile des Hessischen Verfassungsschutzgesetzes (HVSG) sind verfassungswidrig; betrifft engmaschige Überwachung von Mobilfunkgeräten, die Einholung von Reiseinformationen Betroffener, der Einsatz verdeckter Mitarbeitender zur Aufklärung sowie die Weitergabe nachrichtendienstlich erhobener Daten an Strafverfolgungsbehörden.
- OLG Düsseldorf, Urteil vom 31.10.2024, Az. 20 U 51/24, Übermittlung von Positivdaten zur Betrugsprävention und zur Aufrechterhaltung eines zuverlässigen Scoring-Systems stellt ein berechtigtes Interesse der Beklagten dar und ist nach Art. 6 Abs. 1 lit. f) DSGVO gerechtfertigt. Die Interessen der betroffenen Personen überwiegen nicht, da die Übermittlung der Daten nur geringfügige Auswirkungen hat und keine sensiblen Informationen betrifft.
- Der BfDI wurde von der Initiative "European Blockchain Sandbox" als eine der fünf innovativsten Aufsichtsbehörden von 50 teilnehmenden Organisationen ausgezeichnet. Die pan-europäische Initiative der Europäischen Kommission beschäftigt sich mit Anwendungsfällen sogenannter Distributed Ledger Technologies (DLT). Ziel ist es, mehr Rechtssicherheit bei Lösungen zu erreichen, die auf Blockchain-Technologie setzen. Leider finden sich auf der BfDI-Webseite keine weiteren Informationen, so dass man nur raten kann, warum genau, die Behörde als „innovativ“ ausgezeichnet wurde.