Ausgewählte aktuelle Regularien im IT- und Datenschutzrecht

Fokus	Vorschrift	Inkrafttreten am	Anwendung seit	Zielsetzung	Anwenderkreis
Datenschutz	Datenschutzgrundverordnung (DSGVO)	2016	25.05.2018	**Personenbezogene Daten** werden natürlichen Personen zugeordnet. Jede (nicht private) Verarbeitung personenbezogener Daten muss durch • Betroffenen selbst • ein Gesetz oder • berechtigtes Interesse des Verarbeiters **legitimiert** und **dokumentiert** werden.	**Unternehmen**, die Dienstleistungen oder Waren in Deutschland oder der **EU** anbieten und/oder **Mitarbeiter** beschäftigen 1
	Bundesdatenschutzgesetz-Reform (BDSG-Reform)	**Entwurf** 27.03.2024		Institutionalisierung einer **Konferenz der Datenschutzaufsichtsbehörden** des Bundes und der Länder (DSK) Ziel: **Verbesserung der Durchsetzung** des Datenschutzrechts und einer länder- und bundesübergreifenden **Harmonisierung** (einheitliche Praxis) Insbesondere: **neue Regelungen zum Scoring** von Auskunfteien zur Bewertung der Zahlungsfähigkeit	Verarbeitung personenbezogener Daten öffentlicher Stellen des Bundes und der Länder sowie für nichtöffentliche Stellen (u.a. Unternehmen) 2
Recht des Datenzugangs bzw. der Datennutzung	Data Governance Act (Verordnung 2022)	Juni 2022	24.09.2023	Öffentlich finanzierte **Datenerhebungen sollen der Allgemeinheit** für eine individuelle Nutzung zur **Verfügung gestellt** werden. Das Teilen von Daten soll erleichtert werden. **Festlegung von Prozessen und Strukturen für die Zurverfügungstellung sowie den Austausch von Daten** Dazu notwendig: **Rechtsrahmen** für die gemeinsame Nutzung von Daten • neutraler Zugang zu Daten • Sicherung Interoperabilität von Daten • Vermeidung von Lock-in-Effekten	Nutzer Unternehmen Öffentliche Stellen 3
	Data Act (Datengesetz)	2024	11.01.2024	Fairer und verlässlicher Anspruch auf Zugang zu personenbezogenen und nicht-personenbezogenen Daten durch • Einzelpersonen • Unternehmen • Öffentliche Stellen Regelung, **wer unter welchen Bedingungen Datenzugang** erhalten soll. Definition eines Katalogs missbräuchlicher Nutzungsbedingungen	Nutzer Unternehmen Öffentliche Stellen Anbieter von (physischen) Produkten bzw. IoT-Systemen, bei deren Nutzung Daten generiert werden 4
Wettbewerbsrecht und Konsumentenschutz für die digitale Welt	Digital Markets Act (DMA) (Gesetz über digitale Märkte) **(VO (EU) 2022/1925)**	1. November 2022	17.02.2024	Neue EU-Regulierung für besonders mächtige digitale Plattformen Ziel: Stärkung des Wettbewerbs auf digitalen Märkten, um den Missbrauch der Marktmacht durch Tech-Giganten (wie z. B. Alphabet, Amazon, Apple, Meta und Microsoft) zu verhindern Spezialregelungen für Online-Gatekeeper; dürfen **Nutzerdaten nicht dazu nutzen**, um ihre bereits bestehende starke Stellung im Wettbewerb weiter auszubauen	Online-Gatekeeper (google, Amazon, Facebook (Meta), Apple, Microsoft) und anderen Unternehmen über 75 Mrd. EUR Unternehmenswert bzw. **über 7,5 Mrd. EUR Jahresumsatz** 5
	Digital Services Act DSA) Gesetz über digitale Dienste **VO (EU)B 2022/2065**	1. November 2022	17.02.2024 In Deutschland: **Gesetz über digitale Dienste** vom 14.5.2024 (begleitet EU-VO)	**Grundrechte** von Nutzerinnen und Nutzern im Internet werden **umfassender geschützt,** **Illegale Inhalte** können **schneller entfernt** werden. • Anforderungen an Transparenz bei Ausgestaltung der Dienste • Umgang mit rechtswidrigen Inhalten • Anforderungen an Werbung (**Verbot von „dark patterns**“ – bei denen Nutzer zu Entscheidungen verleitet werden können, die sie nicht frei getroffen hätten) • Onlineplattformen und Suchmaschinen mit monatlich mindestens 45 Mio. aktiven Nutzern: besondere Sorgfaltsanforderungen (z. B. Risikoanalyse und Risikominimierung) Bei Verstößen kann EU **Bußgelder** bspw. bis zu einer Höhe von 10 % des weltweiten Jahresumsatzes verlangen.	Online-Vermittlungsdienste Online-Suchmaschinen und Online-Plattformen 6

Fokus	Vorschrift	Inkrafttreten am	Anwendung seit	Zielsetzung	Anwenderkreis
Künstliche Intelligenz	**Artificial Intelligence Act (AI Act) Verordnung** zur Künstlichen Intelligenz	2024	21. Mai 2024 Neue Regeln gelten ab 2026; teilweise schon ab 2025	**Weltweit erstes Gesetz zur Regulierung von KI** AI Act stellt den Mensch in den Vordergrund: • KI-Anwendungen dürfen nicht missbraucht werden • die Grundrechte müssen geschützt werden • Innovationen in Wissenschaft und Wirtschaft müssen gefördert werden **Risikobasierter Ansatz**: Je höher das Risiko einer KI-Anwendung eingestuft wird, desto strenger sind die Vorgaben • **Verbot bestimmter Praktiken** von KI-Systemen (z. B. bei gezielter Beeinflussung des Verhaltens von Personen und deren Manipulation; gezieltes „Social Scoring" – Förderung von erwünschtem Verhalten durch Vergabe von Punkten) • **Transparenzpflicht**: eindeutige Kennzeichnung künstlich erzeugter Inhalte (Audios, Bilder, Videos) • **Regularien für „Hochrisiko-KI"** (z. B. Diagnosesysteme in der Medizin, autonomes Fahren, Systeme der öffentlichen Sicherheit) – Zulassungsvoraussetzungen werden definiert – höhere Pflichten als Anwendungen mit geringem Risiko	**Jedes** Unternehmen, das KI • in Verkehr bringt, • anbietet oder • **nutzt** • und das einen Bezug zur EU hat (entweder in EU ansässig oder die KI-Systeme werden in der EU genutzt) 7
IT-Sicherheit	**Cyber Resilience Act (CRA) VO (EU) 2024/2847**	11.12.2024	Stufenweise: **11.06.2026** Konformitätsbewertungsstellen können die Erfüllung der Anforderungen an den CRA bewerten **11.09.2026** Meldepflicht für Schwachstellen und Sicherheitsvorfälle **11.12.2027** Alle CRA-Anforderungen sind bei neuen Produkten einzuhalten	**NEU**: Erster europäischer Rechtsrahmen zum **Schutz vor Cyberangriffen** Richtlinie zur **Verbesserung des Cybersicherheitsniveaus** für Produkte mit digitalen Elementen **entlang der gesamten Lieferkette** „**Produkte mit digitalen Inhalten**": • Produkte, die **mit einem Gerät oder einem Netzwerk verbunden** werden können, • sowohl **Hardwareprodukte** mit vernetzten Funktionen (z.B. Smartphones, Laptops, Mikroprozessoren, digitale Zutrittskontrollen; vernetzte Sicherheitskameras, 3D-Drucker für Baukomponenten, uvm.) als auch • reine **Softwareprodukte** (z.B. **Buchhaltungssoftware**, Computerspiele, mobile Apps) **Pflichten nach dem CRA**: • bereits bei der **Produktentwicklung** ist Cybersicherheit zu berücksichtigen • **Konformitätserklärung** (Nachweis, dass das Produkt alle Anforderungen des CRA erfüllt) • **Meldepflicht** für aktiv **ausgenutzte Schwachstellen bis hin zu schwerwiegenden Sicherheitsvorfällen** (Einrichtung einer neuen zentralen Meldeplattform) • **Fünfjähriger Supportzeitraum** (Security-Updates müssen dem Endanwender zur Verfügung gestellt werden) **Erleichterungen für KMU** vorgesehen Bei **Verstößen** gegen CRA drohen Bußgelder, Marktzugangsbeschränkungen/-verbote für Produkte, die die CRA-Anforderungen nicht erfüllen, oder der Rückruf bereits verkaufter Produkte	• Hersteller, • Importeure und • Händler, die Produkte mit digitalen Elementen **für den EU-Markt** entwickeln, herstellen oder in der EU in Verkehr bringen 8
	Network and Information Security Richtlinie (NIS-2-Richtlinie) RL (EU) 2022/2555	Januar 2023	Bis 18.10.2024 Umsetzung in nationales Recht noch **Entwurf**: **NIS2UmsuCG: BSIG-E vom 02.10.2024)**	Regelungen der **Sicherheit von Informations- und Kommunikationstechnik** Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union Verpflichtung der Mitgliedstaaten zur **Verabschiedung einer nationalen Cybersicherheitsstrategie**, um die Cybersicherheit und Resilienz der Verwaltung und bestimmter Wirtschaftssektoren zu stärken Anwendungsbereich betrifft insgesamt **18 Industriesektoren:** • Anforderungen an ihr **Risikomanagementsystem und die Cybersicherheit** • 3-stufiges Meldesystem für Sicherheitsvorfälle	Beide Richtlinien **sollen sicherstellen**, dass • als kritisch eingestufte Einrichtungen • die Bevölkerung in der EU • mit lebenswichtigen Gütern und Dienstleistungen versorgen können **18 betroffene Sektoren:** 9
	Critical Entities Resilience Directive Richtlinie (CER)	Januar 2023	Bis 18.10.2024 Umsetzung in nationales Recht noch **Entwurf**: **KRITIS-DachG-E vom 05.11.2024**	Regelung des **physischen Schutzes vor Sabotage und Angriffen** Anwendungsbereich betrifft insgesamt 18 Industriesektoren, an die umfassende Anforderungen an ihr Risikomanagementsystem und die Cybersicherheit gestellt werden	1. Energie 2. Finanzmarktinfrastruktur 3. Trinkwasser 4. Digitale Infrastruktur 5. Forschung 6. Banken 7. Weltraum 8. Verwaltung 9. Abfall 10. Anbieter digitaler Dienste 11. Gesundheit 12. Transport 13. Ernährung 14. Post 15. Abwasser 16. Verwaltung von IKT-Diensten 17. Gefährliche Chemikalien 18. Industrie 10