bitkom

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Telekommunikationsgesetz (TKG)	Z. T. Umsetzung von EU- Vorgaben (insb. EECC)	National	22.06.2004, seitdem zahlreiche Novellen Zuletzt umfassende Änderungen zeitgleich mit der Einführung des TTDSG zum 01.12.2021	Alle Unternehmen oder Personen, die im Geltungsbereich dieses Gesetzes Telekommunikationsnetze oder Telekommunikationsanlagen betreiben oder Telekommunikationsdienste erbringen sowie weitere nach diesem Gesetz Berechtigten und Verpflichteten	▪ Technische und organisatorische Schutzmaßnahmen, § 165 TKG ▪ Bestimmung eines Sicherheitsbeauftragten und Erstellung eines Sicherheitskonzepts, § 166 TKG ▪ Meldepflichten bei Sicherheitsvorfällen/Datenschutzverletzungen, §§ 168, 169 TKG ▪ Gewährleistung der Sicherheit von Daten, § 178 TKG ▪ Notfallvorsorge, § 184 ff. TKG	Geldbuße i.H.v. bis zu 1.000.000 Euro, § 228 VII Nr. 1 TKG Betriebsuntersagung, § 183 IV TKG	V	BNetzA (§ 191 TKG)	▪ DS-GVO in Bezug auf personenbezogene Daten ▪ E-Evidence hinsichtlich der Zugriffe von Strafverfolgungsbehörden zur Sicherung von Beweismitteln ▪ Art. 10-Gesetz und StPO mit Blick auf die Überwachung von Telekommunikation (§ 170 TKG)
Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)	Z. T. Umsetzung von EU-Vorgaben	National	01.12.2021	Alle Unternehmen und Personen im Anwendungsbereich des Gesetzes, insb. Anbieter von TK-Diensten und Telemedien sowie Betreiber von Telekommunikationsanlagen und öffentlichen Telekommunikationsnetzen	▪ Wahrung des Fernmeldegeheimnisses, § 3 TTDSG ▪ Regelungen zu Verkehrs- und Standortdaten, § 9 ff. TTDSG ▪ Verpflichtung zum Treffen technischer und organisatorischer Vorkehrungen für Anbieter von Telemedien, § 19 TTDSG	Freiheits- oder Geldstrafe nach § 27 TTDSG, Bußgeld bis zu 300.000 € nach § 28 TTDSG	V	BfDI (§ 29 TTDSG), BNetzA (§ 30 TTDSG)	▪ TKG in Bezug auf Anbieter von TK-Diensten ▪ TMG für Anbieter von Telemedien ▪ DS-GVO hinsichtlich Datenverarbeitung

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflich-tend/ freiwillig (V/F)	Zuständi-ge Behörden	Wechselwirkung zwischen den Gesetzen
Richtlinie zur Netz- und Informati-onssicherheit (NIS-RL)	RL	EU	29.06.2016 Neue Version (»NIS 2.0«) aktuell zur Billigung beim Rat und im Parlament)	MS; Betreiber wesentlicher Dienste und Anbieter digitaler Dienste Vrs. Änderungen in NIS 2.0-Richtlinie: ▪ Unterscheidung in »Essential Entities« und »Important Entities« ▪ Grds. Erfassung aller mittleren und großen Unterneh-men, Ausnahme von Kleinst- und kleine Unternehmen mit Rückausnahmen ▪ Ausweitung der erfassten Sektoren (z. B. um Abwasser, öff. Verwaltung, Weltraum)	▪ Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen ▪ Schaffung einer Kooperationsgruppe, zur strategi-schen Zusammenarbeit der Mitgliedstaaten ▪ Schaffung eines Netzwerks von Computer-Notfall-teams (CSIRTs-Netzwerk Computer Security Incident Response Teams Network) ▪ Sicherheitsanforderungen und Melde- pflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste ▪ Benennung nationaler zuständiger Behörden, zentraler Anlaufstellen und CSIRTs Vrs. Neuerungen in NIS 2.0: ▪ Maßnahmenkatalog mit technischen, operativen und organisatorischen Maßnahmen ▪ Ausweitung & Konkretisierung der Meldepflichten ▪ Risikobewertung von Lieferketten ▪ europäisch koordinierte Datenbank zur Offenle-gung von Schwachstellen	Mitgliedstaaten erlassen Vorschriften über wirksame, angemessene und abschreckende Sanktionen für Verstöße In DE: Bußgeld in Höhe von bis zu 2 Millionen EURO, § 14 BSIG Vrs. Änderungen durch NIS 2.0: Geldbußen in Höhe von mindestens 10 Millionen EUR oder bis zu 2 % des gesamten weltweiten Jahresum-satzes des Unterneh-mens	V	EU: ENISA DE: BSI	▪ CER-RL ▪ EECC/TKG ▪ CSA ▪ DORA

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
BSI-Gesetz (BSIG), BSI-KritisVO		National Dient u. a. Umsetzung der NIS-RL	20.08.2009 (BSIG); 03.05.2016 (BSI-KritisV) Zuletzt umfassende Änderungen am 18. Mai 2021 durch IT-Sicherheitsgesetz 2.0	Betreiber Kritischer Infrastrukturen: ▪ Finanzen und Versicherung ▪ Gesundheit ▪ Transport und Verkehr ▪ Energie ▪ IT und Tele-kommunikation ▪ Wasser ▪ Ernährung Unternehmen im besonderen öffentlichen Interesse Anbieter digitaler Dienste	▪ Treffen von organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen kritischer Infrastrukturen, § 8a Abs. 1, 1a BSIG; ab 01. Mai 2023 Einsatz von Systemen zur Angriffserkennung; Nachweispflicht gemäß Abs. 3 ▪ Registrierung und Meldung einer Kontaktstelle beim BSI, § 8b Abs. 3 BSIG ▪ Meldung von Störungen/Sicherheitsvorfällen an das BSI, §§ 8b Abs. 4, 8c Abs. 3, 8f Abs. 7, 8 BSIG ▪ Treffen technischer und organisatorischer Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme zur Bereitstellung digitaler Dienste, § 8c Abs. 1 BSIG ▪ Selbsterklärung zur IT-Sicherheit für Unternehmen im bes. öff. Interesse, Registrierung und Meldung einer erreichbaren Stelle, § 8f Abs. 1, 5 BSIG ▪ Untersagung des Einsatzes Kritischer Komponenten nicht vertrauenswürdiger Hersteller, § 9b BSIG ▪ Freiwilliges IT-Sicherheitskennzeichen, § 9c BSIG	Bußgelder in Höhe von bis zu 20 Millionen €, § 14 BSIG	V F (IT-Sicherheitskennzeichen)	BSI	▪ NIS-RL ▪ CER-RL ▪ CSA ▪ TKG/EECC

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Rechtsakt zur Cybersicherheit/EU Cybersecurity Act (CSA)	VO	EU	27.06.2019 bzw. 28.06.2021	MS/NISA/Hersteller bzw. Anbieter von IKT-Produkten, -Diensten und -Prozessen	▪ EU-weiter Rahmen zur Zertifizierung von IT-Sicherheit ▪ Ständiges Mandat für die europäische Cyber-Sicherheitsbehörde ENISA ▪ Ausarbeitung verschiedener Cybersicherheitszertifizierungen (durch die ENISA), z. B. Candidate Cybersecurity Certification Scheme (EUCC), Cloud Services Scheme (EUCS) ▪ Ernennung einer nationalen Behörde für die Cybersicherheitszertifizierung & Festlegung deren Aufgaben	Mitgliedstaaten erlassen Vorschriften über wirksame, angemessene und abschreckende Sanktionen für Verstöße	V/F (Cybersicherheitszertifizierungen sind freiwillig, solange nicht anderweitig eine Pflicht festgeschrieben wird)	ENISA, BSI (= nationale Behörde für Cybersicherheitszertifizierung)	BSIG, BSI-KritisVO
Datenschutz-Grundverordnung (DS-GVO)	VO (+parallele RL für Polizei und Justiz)	EU	25.05.2018	Alle, die i. S. d. VO personenbezogene Daten verarbeiten, Art. 2 DSGVO	▪ Treffen technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung, Art. 32 DSGVO ▪ Meldung von Verletzungen des Schutzes personenbezogener Daten, Art. 33 DSGVO	Umfassende Befugnisse der Aufsichtsbehörden, z. B. ▪ Beschränkung oder Verbot der Verarbeitung, Art. 58 Abs. 2 lit. f DSGVO ▪ Geldbuße in Höhe von bis zu 20 Millionen €, Art. 83 DSGVO	V	EDPB, nationale DPA	E-Privacy-VO BDSG TKG TTDSG

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflich-tend/ freiwillig (V/F)	Zuständi-ge Behörden	Wechselwirkung zwischen den Gesetzen
Bundesda-tenschutzge-setz (BDSG)	Ergän-zung zur SGVO	National	30.06.2017	Alle, die i. S. d. Gesetzes personenbezogene Daten verarbeiten, § 1 BDSG	▪ Treffen technischer und organisatorischer Maß-nahmen zur Gewährleistung der Sicherheit der Verarbeitung, § 64 BDSG ▪ Meldung von Verletzungen des Schutzes perso-nenbezogener Daten, § 65 BDSG	Insb. Schadensersatz/ Entschädigung, § 83 BDSG			DSGVO E-Privacy-VO TKG TTDSG
E-Evidence	VO und RL	EU	Derzeit offen, Finalisierung 2022 möglich	MS	▪ Datenherausgabe/Datensicherung ▪ EU-ausländische Strafverfolgungsbe- hörden sollen ermächtigt werden, direkt beim nationalen Provider die Datenher- ausgabe/Datensicherung anzuordnen ▪ Fristen: 6 Stunden bis 10 Tage ▪ Prüfungspflichten der Provider ▪ Bestellung eines verantwortlichen Vertreters innerhalb der EU nach RL	▪ MS werden verpflichtet, für Verstöße gegen die Verpflichtun-gen aus den Artikeln 9, 10 und 11 E-Evi- dence VO zu bestimmen (wirksam, verhält-nismäßig und abschreckend) ▪ Ebenso bei Verstößen gegen die Pflicht einen verantwortlichen Vertreter innerhalb der Union zu bestimmen nach E-Evidence RL	V	Strafver-olgungs-behörden	E-Privacy-VO DS-GVO
E-Privacy-Verordnung	VO	EU	Derzeit offen	Vrs. Unternehmen der Digitalwirtschaft	[...]	Wie DS-GVO	V	EDPB, nationale DPA	DS-GVO BDSG TTDSG

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Richtlinie über die Resilienz kritischer Einrichtungen (CER-RL)	RL	EU	Derzeit offen	MS	▪ Verpflichtung der Mitgliedstaaten zur Verabschiedung einer Resilienzstrategie für kritische Einrichtungen, Art. 3, sowie Unterstützung kritischer Einrichtungen bei der Verbesserung ihrer Resilienz ▪ Erstellung einer Liste wesentlicher Dienste und Bewertung der Risiken bei deren Erbringung ▪ Ermittlung kritischer Einrichtungen, Art. 5 ▪ Festlegung von Verpflichtungen kritischer Einrichtungen zur Verbesserung deren Resilienz und Fähigkeit, ihre Dienste zu erbringen, Art. 10 ff. ▪ Aufsicht und Durchsetzungsmaßnahmen gegenüber kritischen Einrichtungen, Art. 16 ff.	Mitgliedstaaten erlassen Vorschriften über wirksame, verhältnismäßige und abschreckende Sanktionen	V	»Gruppe für die Resilienz kritischer Einrichtungen«, Kommission	BSIG, BSI-KritisVO CSA NIS-RL
Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA)	VO	EU	Offen, derzeit im Rat/ Parlament	Finanzunternehmen	Festlegung einheitlicher Anforderungen für die Sicherheit von Netz- und Informationssystemen, die die Geschäftsprozesse von Finanzunternehmen unterstützen	Mitgliedstaaten legen geeignete verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen für Verstöße fest	V	Diverse, festgelegt in Art. 41 des Entwurfs	NIS-RL BSIG, BSI-KritisV CSA

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Cyber-Resilience Act	VO	EU	Vorstellung im September 2022	Hersteller von Produkten mit digitalen Elementen; MS	▪ Gewährleistung der Sicherheit von Produkten mit digitalen Elementen während des gesamten Lebenszyklus (»cybersecurity by design«) ▪ Gewährleistung eines kohärenten Rahmens für die Cybersicherheit, der den Herstellern von Hardware und Software die Einhaltung der Compliance-Vorgaben erleichtert ▪ Verbesserung der Transparenz der Sicherheitseigenschaften von Produkten mit digitalen Elementen ▪ Befähigung von Unternehmen und Verbrauchern, Produkte mit digitalen Elementen sicher zu nutzen	Geldbußen von bis zu 15.000.000 EUR oder in Höhe von bis zu 2,5 % des gesamten weltweiten Jahresumsatzes im vorausgegangenen Geschäftsjahr	V		CSA
Richtlinie über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Open Data und PSI-Richtlinie) (EU 2019/1024)	RL	EU	16.07.2019	MS	▪ Private Unternehmen sollen Informationen, die bei öffentlichen Stellen wie Ämtern, Behörden oder Bibliotheken vorliegen, kostengünstig oder kostenfrei elektronisch zur Verfügung gestellt bekommen, um damit Wirtschaftswachstum anzuregen und neue Geschäftsmodelle zu ermöglichen ▪ Die Richtlinie soll auch bereits öffentlich zugängliche Forschungsdaten, die aus öffentlich geförderter Forschung stammen, erfassen	keine	V		

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflich-tend/ freiwillig (V/F)	Zuständi-ge Behörden	Wechselwirkung zwischen den Gesetzen
Europäischer Kodex für die elektronische Kommunika-tion (EECC)	RL	EU	20.12.2018	MS	▪ Errichtung eines Binnenmarkts für elektronische Kommunikationsnetze und -dienste (Interoperabilität) ▪ Ausbau und Nutzung von Netzen mit sehr hoher Kapazität ▪ Gewährleistung der Zugänglichkeit und Sicherheit von Netzen und Diensten ▪ Einführung öffentlicher Warnsysteme, um die Bevölkerung in Krisengebieten per Handy alarmie-ren zu können ▪ Gewährleistung der Sicherheit von elektronischen Kommunikationsnetzen und -diensten durch angemessene und verhältnismäßige technische und organisatorische Maßnahmen nach dem Stand der Technik, Art. 40 Abs. 1 EECC ▪ Unverzügliche Meldung von Sicherheitsvorfällen, Art. 40 Abs. 2 EECC ▪ Information potenziell betroffener Nutzer über alle möglichen Schutz- und Abhilfemaßnahmen im Falle einer besonderen oder erheblichen Gefahr eines Sicherheitsvorfalls, Art. 40 Abs. 3 EECC ▪ Sicherstellen der Anwendung und Durchsetzung von Weisungen der Mitgliedstaaten und zuständi-ger Behörden an Anbieter elektronischer Kommu-nikationsnetze/-dienste, Art. 41 EECC	keine	V	ENISA	DSGVO TKG TTDSG CSA NIS-RL BSIG, BSI-KritisVO CER-RL

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (Free Flow of Data-VO)	VO	EU	Verbindliche Anwendung EU-weit seit 28.05.2019	MS	Datenlokalisierungsvorgaben, Ausnahmen bei Gründen öffentlicher Sicherheit	Die Mitgliedstaaten können wirksame, verhältnismäßige und abschreckende Sanktionen verhängen	V		
Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS Verordnung)	VO	EU	17.09.2014/ 01.07.2016	MS; Vertrauensdiensteanbieter	▪ Festlegung von Sicherheitsniveaus elektronischer Identifizierungssysteme, Art. 8 eIDAS-VO ▪ Ergreifen geeigneter technischer und organisatorischer Maßnahmen nach dem neuesten Stand der Technik; Information der Beteiligten über die nachteiligen Folgen von Vorfällen, Art. 19 Abs. 1 eIDAS-VO ▪ Unverzügliche Meldung von Sicherheitsverletzungen und Integritätsverlusten an zuständige Stellen und ggf. betroffene jur. & nat. Personen, Art. 19 Abs. 2 eIDAS-VO ▪ Anforderungen an (qualifizierte) Vertrauensdienste und elektronische Signaturen ▪ Regelungen zu elektronischen Siegeln, Zeitstempeln, Einschreiben, Dokumenten und zu Website-Authentifizierung	keine	V	BNetzA, BSI (für Zertifikate für die Website-Authentifizierung), BMWK, BMI	VDG, VDV DSGVO

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
eIDAS 2.0	VO	EU	Veröffentlichung eines Entwurfs für Oktober 2022 geplant	MS; Vertrauendsdienstanbieter	▪ MS sollen verpflichtet werden, eine digitale Brieftasche (EU Digital Identity Wallet) anzubieten, die Grundlage für die eID sein und qualifizierte elektronische Signaturen & Siegel erstellen soll ▪ Zu den Vertrauensdiensten sollen künftig auch qualifizierte Archivierungsdienste gehören ▪ Definiert werden auch entsprechende Sicherheitsniveaus für diese Dienste		V		
Vertrauensdienstegesetz (VDG), Vertrauensdienste-verordnung (VDV)		National	29.07.2017/ 28.08.2019	Vertrauensdiensteanbieter in Deutschland	▪ Anpassung alter Rechtslage (insb. Signaturgesetz) an eIDAS-VO ▪ Mitwirkungspflichten von Vertrauensdiensteanbietern bei Überprüfungen, § 5 VDG ▪ Sonstige Vorschriften für qualifizierte Vertrauensdienste und qualifizierte elektronische Signaturen, §§ 9 ff. VDG	Betriebsuntersagung, § 4 Abs. 3; Geldbuße bis zu 100.000 €, § 19 VDG	V	BNetzA; BSI (für Zertifikate für die Website-Authentifizierung)	eIDAS-VO DSGVO/BDSG
IT-Strafrecht im Strafgesetzbuch (StGB)		National	Fortlaufend novelliert, relevanter IT-Bezug insb. seit August 2007	Bürger	▪ § 202a-d StGB – unrechtmäßig Erlangen von Informationen aus IT-Systemen (Hackerparagraph § 202c) ▪ § 263a StGB – Computerbetrug ▪ § 269 StGB – Fälschung beweiserheblicher Daten ▪ § 270 StGB – Täuschung im Rechtsverkehr bei Datenverarbeitung ▪ § 303a/b StGB – unrechtmäßige Zerstörung von Computern/Daten	Freiheitsstrafe oder Geldstrafe, je nach Delikt	V	BMJ Strafverolgungsbehörden	

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Strafprozessordnung (StPO)		National	01.04.1987 Quellen-TKÜ zuletzt maßgeblich angepasst durch das Gesetz zur Anpassung des Verfassungsschutzrechts vom 05.07.2021	Strafverfolgungsbehörden	▪ Regelungen zur Telekommunikationsüberwachung, insb. auch durch Eingriff in informationstechnische Systeme (sog. Quellen-TKÜ), § 100a StPO ▪ Online-Durchsuchung, § 100b StPO	Unverwertbarkeit bei Verstößen der Strafverfolgungsbehörden, z. B. § 110d StPO	Maßnahmen im Ermessen der Behörden mit richterlicher Anordnung	StA Polizei Gerichte	Art. 10-Gesetz E-Evidence
Artikel 10-Gesetz		National	27.06.2001 Zuletzt Änderungen durch das Gesetz zur Anpassung des Verfassungsschutzrechts vom 05.07.2021	Anbieter von Post- und Telekommunikationsdiensten	Regelungen zu Auskunft über und Überwachung von Telekommunikation, insb. Eingriff in informationstechnische Systeme, §§ 2 Abs. 1a, 11 Abs. 1a Art. 10-Gesetz	Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bei Verstoß gegen Mitteilungsverbote, § 17, 18 Art. 10-Gesetz Geldbuße bis zu 15.000 €, § 19 Art. 10-Gesetz	V	Verfassungsschutzbehörden; MAD; BND; BMI	TKG E-Evidence

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
					Weitere Themen				
Gesetz zum bes-seren Schutz von Geschäftsgeheimnissen (GeschGehG)	Umsetzung der now-How-Schutz-RL	National (Umsetzung der Know-How-Schutz. Richtlinie)	26.04.2019		▪ Verbot der Erlangung, Nutzung oder Offenlegung von Geschäftsgeheimnissen, § 4 GeschGH ▪ Ausnahmen u. a. für Wistleblower und Journalisten (§ 5 GeschGehG)	Ordnungsgeld bis zu 100 000 Euro oder Ordnungshaft bis zu sechs Monaten, § 17 GeschGH Freiheitsstrafe bis zu fünf Jahren, § 23 GeschGH	V		UWG, aber GeschGehG lex specialis
Urheber-rechtliche-Schutz von Software gemäß UrhG		National	Letzte Novellierung 28.11.2019		▪ § 69a ff. UrhG – Urheberrechtlicher Schutz für Computerprogramme ▪ § 95a UrhG – Verbot der Umgehung technischer Maßnahmen zum Schutz eines geschützten Werkes/Schutzgegenstandes	▪ § 97 UrhG – Unterlassung und Schadensersatz ▪ § 98 UrhG – Vernichtung, Rückruf und Überlassung ▪ § 100 UrhG – Entschädigung ▪ § 101 UrhG – Anspruch auf Auskunft ▪ § 101a Anspruch auf Vorlage und Besichtigung	V		
Messstellen-betriebsgesetz (MsbG)		National	30.08.2016		Anforderungen an Zertifizierung von Smart Meter Gateway/Zähler, basierend auf IT-Sicherheit und Datenschutz			BNetzA	

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Richtlinie über die Bereitstellung von Funkanlagen auf dem Markt (Radio Equipment Directive - RED-RL)	RL	EU	12. Juni 2014	MS	▪ Funkanlagen müssen den Schutz der Gesundheit und Sicherheit von Menschen und Haus- und Nutztieren sowie den Schutz von Gütern gewährleisten ▪ Funkanlagen dürfen weder schädliche Auswirkungen auf das Netz oder seinen Betrieb haben noch eine missbräuchliche Nutzung von Netzressourcen, wodurch eine unannehmbare Beeinträchtigung des Dienstes verursacht würde, bewirken ▪ Funkanlagen müssen über Sicherheitsvorrichtungen verfügen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden ▪ Funkanlagen müssen bestimmte Funktionen unterstützen zum Schutz vor Betrug ▪ Art. 16 ff. RED – Konformitätsbewertung von Funkanlagen	Mitgliedstaaten legen Regeln für Sanktionen fest	V	BNetzA (BMWK) (Kontrolle durch Marktüberwachungsbehörden)	CSA FuAG
Gesetz über die Bereitstellung von Funkanlagen auf dem Markt (FuAG)	Dient der Umsetzung der RED-RL	National	28.06.2017	Hersteller, Einführer und Händler von Funkanlagen	Entsprechend der RED-RL	Zwangsgeld von bis zu 500000 € zur Durchsetzung von Anordnungen der BNetzA, § 34 FuAG Geldbuße bis zu einhunderttausend Euro, § 37 FuAG	V	BNetzA	RED-RL

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Richtlinie über die allgemeine Produktsicherheit	RL	EU	15.01.2002 Zuletzt Überarbeitungsvorschläge der Kommission vom 30.06.2021	MS	▪ Es dürfen nur »sichere« Produkte entsprechend spezieller Vorschriften in den Verkehr gebracht werden, Art. 5 ▪ Information von Verbrauchern über Gefahren von Produkten, Art. 5 Inhalt des Überarbeitungsvorschlags: ▪ Aktualisierung der Definition des Begriffs »Produkt« (»any item, interconnected or not to other items(...)«) und spezifische Definition des Begriffs »Online-Marktplatz« ▪ Übergang der Verantwortung für ein Produkt auf die Person, die daran »wesentliche Änderungen« vornimmt ▪ Neue Sicherheitsaspekte zur Bewertung der Produktsicherheit, z. B. mögliche Risiken im Zusammenhang mit Produkten, die auf neuen Technologien basieren (z. B. Cybersecurity-Risiken) ▪ Spezifische Verpflichtungen für Online-Marktplätze (z. B. Entfernung illegaler Produkte über deren Websites innerhalb von zwei Arbeitstagen) ▪ Das RAPEX-System ist jetzt das »Safety Gate«; spezifischere Fristen, um Produktrückrufe effektiver zu machen ▪ erweitertes Recht von Verbrauchern auf Informationen und Rechtsbehelfe ▪ Die Kommission wird in die Lage versetzt, Formen der Zusammenarbeit mit Drittländern zu etablieren, um die Produktsicherheit zu verbessern (z. B. durch die Gewährung einer Teilnahme am Safety Gate usw.)	Mitgliedstaaten legen Sanktionen für Verstöße fest	V		▪ RED-RL/FuAG ▪ Maschinen-RL

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Richtlinie über Maschinen	Bisher RL, soll VO werden	EU	29.06.2006 Vorschlag für neue Maschinen-verordnung am 21.0.2021 veröffentlicht	MS	▪ Erfüllung grundlegender Sicherheits- und Gesundheitsschutzanforderungen vor Inverkehrbringen einer Maschine, Art. 5 ▪ Konformitätsbewertungsverfahren für Maschinen, Art. 12 Neuerungen im Entwurf einer neuen Verordnung: ▪ Link zum Cybersecurity Act ▪ Zu den Maschinenprodukte mit hohem Risiko zählen jetzt auch: Software, die Sicherheitsfunktionen gewährleistet, einschließlich KI-Systeme und Maschinen mit eingebetteten KI-Systemen, die Sicherheitsfunktionen gewährleisten ▪ Änderungen bei der technischen Dokumentation, z. B. muss der Quellcode oder die programmierte Logik der sicherheitsbezogenen Software zum Nachweis der Konformität des Maschinenprodukts angegeben werden Neu im Scope: ▪ Maschinen, bei denen nur der Upload einer für ihre spezifische Anwendung bestimmten Software fehlt ▪ »Sicherheitsbauteil« ist eine physische oder digitale Komponente, einschließlich Software, einer Maschine	Mitgliedstaaten legen Sanktionen für Verstöße fest	V	BMAS (Kontrolle durch Marktüberwachungsbehörden)	▪ Cybersecurity Act ▪ Künftig ggf. AI-Act

Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Regulierung	VO oder RL	National oder EU	Inkrafttreten	Adressaten	Auswirkungen/Pflichten	Sanktionen	Verpflichtend/ freiwillig (V/F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Digitale Inhalte-Richtlinie & Richtlinie über bestimmte vertragsrechtliche Aspekte des Warenkaufs	RL	EU	20.05.2019	MS	▪ Die Digitale Inhalte-Richtlinie betrifft die Bereitstellung digitaler Inhalte und umfasst u. a. Daten, die in digitaler Form produziert und bereitgestellt werden sowie Dienste, die die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form ermöglichen ▪ Die Richtlinie über bestimmte vertragsrechtliche Aspekte des Warenkaufs betrifft alle Warenverkäufe, unabhängig davon, ob sie physisch (in Geschäften), online oder im Fernabsatz erfolgen ▪ Umfasst insbesondere die Pflicht, Verbraucher über (Sicherheits-)Aktualisierungen für Waren mit digitalen Elementen, digitalen Inhalte und digitalen Dienstleistungen zu informieren und diese bereitzustellen (umgesetzt in § 327e Abs. 3, 327f, 475b Abs. 4, 475c BGB)	Mängelrechte des (Verbraucher-)-Käufers	V		
Richtlinie über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen	RL	EU	8.12.2008 Aktuell in Revision, parallel zur NIS-Review	MS	▪ Umfasst zum jetzigen Zeitpunkt ausschließlich die Sektoren Energie und Transport ▪ Fokus liegt auf der Gefahr durch Terrorangriffe				NIS Richtlinie
UN/ECE (Economic Commission for Europe) Regelungen	R1-R152	UN/EU National	Fortlaufende Weiterentwicklung	Mobilitätssektor	▪ (Internationale) Harmonisierung der technischen Vorschriften für Kraftfahrzeuge ▪ Fragen rund um Automatisierung, Vernetzung und weitere Aspekte rund um die Mobilität der Zukunft			BMDV	

Herausgeber

Bitkom e.V.
Albrechtstraße 10
10117 Berlin

Ansprechpartner

Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit
M +49 151 17439698

Gestaltung

Anna Stolz

Bildnachweis

Titelbild © kviktor | www.stock.adobe.com

Impressum

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom