Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Stand: Juli 2020

bitkom

Herausgeber

Bitkom e.V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Sebastian Artz | Referent IT-Sicherheit
M +49 151 27631531

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
					Kernthemen				
Telekommunikationsgesetz (TKG)	Z. T. Umsetzung von EU-Vorgaben	National	22.06.2004, seitdem zahlreiche Novellen Nächste TKG-Novelle / Umsetzung des EECC bis Ende 2020	Betreiber von öffentlichen Telekommunikationsnetzen und die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten	▪ § 109 TKG – Technische Schutzmaßnahmen ▪ § 109a TKG – Daten- & Informationssicherheit ▪ § 113d TKG – Gewährleistung und Sicherheit der Daten ▪ § 113e TKG – Protokollierung ▪ §113f TKG – Anforderungskatalog ▪ 113 g TKG – Sicherheitskonzept	Z. B. nach § 115 II 1 Nr.1: 500.000 Euro Z. B. nach §126 III: Betriebsuntersagung	V	BNetzA (§116 TKG)	▪ DS-GVO hinsichtlich Datenverarbeitung ▪ E-Evidence hinsichtlich der Zugriffe von Strafverfolgungsbehörden zur Sicherung von Beweismitteln ▪ ePrivacy-Verordnung in Bezug auf Fernmeldegeheimnis und kommunikationsspezifischen Datenschutz ▪ Verfassungsschutzgesetz mit Blick auf die Quellen-TKÜ
Telemediengesetz (TMG)	Z. T. Umsetzung von EU-Vorgaben, z. B. ePrivacy RL	National	26.02.2007, seitdem zahlreiche Novellen	Anbieter von Telemedien	▪ Mit Blick auf IT-Sicherheit muss insb. § 13 Abs. 7 TMG beachtet werden		V	Datenschutzaufsichtsbehörden An den Schnittstellen zum TKG: BNetzA Hinsichtlich Medien: Landesmedienanstalten	▪ ePrivacy Richtlinie (und zukünftig ePrivacy VO) ▪ DS-GVO
Verfassungsschutzgesetz (Artikelgesetz)		National	Kabinettvorlage im Juli 2020	Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten	▪ Regelung der Quellen-TKÜ (durch Änderungen insb. der §§ 2 und 11 G 10)		V	Nationale Sicherheitsbehörden, BMI	▪ TKG sowie z.T. mit dem IT-SiG 2.0

bitkom

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
NIS RL	RL	EU	29.06.2016 Vorzeitige Überarbeitung der NIS RL in Q4 2020 (öffentliche Konsultation bis Oktober 2020)	MS	▪ Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen ▪ Schaffung einer Kooperationsgruppe, zur strategische Zusammenarbeit der Mitgliedstaaten ▪ Schaffung eines Netzwerks von Computer-Notfallteams (CSIRTs-Netzwerk – Computer Security Incident Response Teams Network) ▪ Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste ▪ Benennung nationaler zuständigen Behörden, zentraler Anlaufstellen und CSIRTs	Die Mitgliedstaaten erlassen Vorschriften über Sanktionen für Verstöße	V	Nationale Sicherheitsbehörden, BSI	▪ IT-SiG 2.0 mit Blick auf KRITIS-Sektoren ▪ ECI-Richtlinie hinsichtlich kritischer Infrastrukturen im Allgemeinen ▪ Parallele Überarbeitung der NIS- und ECI-Richtlinie in 2020
IT Sicherheitsgesetz (Artikelgesetz, Auswirkung auf: TKG, TMG, StGB, StPO, BSI-Gesetz)		National Umsetzung der NIS RL	30.06.2017, seit 10.05.2018 für Anbieter digitaler Dienste	Betreiber folgender wesentlicher Dienste: ▪ Finanzen und Versicherung ▪ Gesundheit ▪ Transport und Verkehr ▪ Energie ▪ IT und Telekommunikation ▪ Wasser ▪ Lebensmittel	▪ Unternehmen die als KRITIS (also oberhalb der definierten Schwellenwerte gemäß Anhänge 1 - 7 BSI Kritis-Verordnung) definiert sind, unterliegen besonderer Meldepflichten nach § 8b (3) BSIG und müssen ein definiertes Mindestmaß an IT-Sicherheit einhalten (Stand der Technik nach § 8a (1) BSIG ▪ Nach BSI Kritis-Verordnung sind die Sektoren: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen ▪ Digitale Diensteanbieter, da diese in einer Voll-Harmonisierung aus der NIS-Richtlinie resultieren	In § 14 des Bundesgesetzes sind Bußgelder bis zu 50.000 EUR vorgesehen	V	BSI	
IT Sicherheitsgesetz 2.0		National	Befindet sich in Ressortabstimmung		▪ Ausweitung des Anwendungsbereichs von KRITIS-Regulierungen auf den neuen KRITIS-Sektor „Entsorgung“Einführung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“ sowie des Begriffs „Kritische Komponenten“ ▪ Untersagung des Einsatzes Kritischer Komponenten nicht vertrauenswürdiger Hersteller (§ 9b) ▪ Freiwilliges IT-Sicherheitskennzeichen ▪ Kompetenz- und Befugnisausweitung des BSI, u.a. im Bereich Verbraucherschutz	Gemäß des neugefassten § 14 könnten Verstöße mit Bußgeldern von bis zu 20 Millionen Euro oder von zwei respektive vier Prozent des weltweiten Jahresumsatzes geahndet werden	V (KRITIS Erweiterung) und F (IT-Sicherheitskennzeichen)	BSI, BMI	Überlappung mit der NIS-Review und der Überarbeitung der ECI-RL sowie z.T. mit dem Cybersecurity Act

bitkom

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
EU Cybersecurity Act	VO	EU	27.06.2019	MS / Unternehmen die auf dem Europäischen Markt verkaufen möchten	▪ EU-weiter Rahmen zur Zertifizierung von IT-Sicherheit ▪ Ständiges Mandat für die europäische Cyber-Sicherheitsbehörde ENISA ▪ Ausarbeitung verschiedener Certification Schemes (durch die ENISA). Aktuell diskutiert: der Common Criteria based European cybersecurity certification scheme (EUCC). Ebenfalls in 2020: Scheme on Cloud-Services	Keine Sanktionsmechanismen, da freiwillig	F	BSI, ENISA	Anerkennung von Zertifikaten gemäß CSA wird im Kontext des IT-SiG 2.0 diskutiert
Datenschutz-grundverordnung (DS-GVO)	VO (+parallele RL für Polizei und Justiz)	EU	25.05.2018	MS	▪ […], Datensicherheit insb. Art. 32 ▪ Im Nov 2019 hat der EDPB einen ersten Entwurf der *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* veröffentlicht	Art. 83/84 DS-GVO	V	EDPB, nationale DPA	E-Privacy & E-Evidence
1. und 2. DSAnpUG	Nationale Umsetzung DS-GVO	National	1. DSAnpUG: 25.05.2018 DSAnpUG: 26.11.2019	»Verantwortliche« im Sinne des DS-Rechts	▪ DSAnpUG insb. Anpassung des nationalen Bundesdatenschutzgesetzes an die DSGVO ▪ DSAnpUG Anpassung von über 150 Fachgesetzen an die DSGVO	Richten sich nach DS-GVO	V	Nationale DPAs	
E-Evidence	VO und RL	EU	Derzeit offen, EP-Befassung und Trilog stehen noch bevor	MS	▪ Datenherausgabe/Datensicherung ▪ EU-ausländische Strafverfolgungsbehörden sollen ermächtigt werden, direkt beim nationalen Provider die Datenherausgabe/ 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 Verpflichtungen aus den Artikeln 9, 10 und 11 E-Evidence VO zu bestimmen (wirksam, verhältnismäßig und abschreckend) ▪ Ebenso bei Verstößen gegen die Pflicht einen verantwortlichen Vertreter innerhalb der Union zu bestimmen nach E-Evidence RL	V	Strafverfolgungsbehörden	E-Privacy & DS-GVO
E-Privacy	VO	EU	Derzeit offen	MS	[…]	Wie DS-GVO	V	EDPB, nationale DPA	E-Evidence & DS-GVO

bitkom

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
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		V		
European Electronic Communication Code (EECC)	RL	EU	20.12.2018 Umsetzung in nationales Recht bis spätestens zum 21.12. 2020 (TKG-Novelle)	MS	▪ Errichtung eines Binnenmarkts für elektronische Kommunikationsnetze und –dienste (Interoperabilität) ▪ Ausbau und Nutzung von Netzen mit sehr hoher Kapazität ▪ Gewährleitstung der Zugänglichkeit und Sicherheit von Netzen und Diensten ▪ Einführung öffentlicher Warnsysteme, um die Bevölkerung in Krisengebieten per Handy alarmieren zu können				DSGVO
Free Flow of Data	VO	EU	Verbindliche Anwendung EU-weit seit 28.05.2019	MS	Datenlokalisierungsvorgaben, Ausnahmen bei Gründen öffentlicher Sicherheit	Art. 5 Absatz 4: Die Mitgliedstaaten können in Übereinstimmung mit dem Unionsrecht oder dem nationalen Recht wirksame, verhältnismäßige und abschreckende Sanktionen verhängen, wenn gegen eine Verpflichtung zur Bereitstellung von Daten verstoßen wird	V		
eIDAS Verordnung	VO	EU	01.07.2016	MS	Europaweit einheitliche Regelungen zu elektronischer Identifizierung und elektronischen Vertrauensdiensten		V	BNetzA, BSI, BMWi, BMI	

bitkom

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
Vertrauensdienste-gesetz (VDG)		National	29.07.2017	Vertrauens-diensteanbieter in Deutschland	Anpassung alter Rechtslage (insb. Signaturgesetz) an eIDAS VO		V		
Vertrauensdienste-verordnung (VDV)		National	28.02.2019	Vertrauens-diensteanbieter in Deutschland	Anpassung alter Rechtslage (insb. Signaturverordnung) an eIDAS VO		V		
IT-Recht im Strafgesetzbuch (StGB)		National	Fortlaufend novelliert, relevanter IT-Bezug insb. seit August 2007		▪ §§ 202a-c StGB – unrechtmäßig Erlangen von Informationen aus IT-Systemen (Hackerparagraph § 202c) ▪ § 263a StGB – Computerbetrug ▪ §§ 303a/b StGB – unrechtmäßige Zerstörung von Computern / Daten	§§ 269 und 270 StGB – Ahndung von Identitätsdiebstahl		BMJV	
					Randthemen				
Know-How-Schutz-Richtlinie (2016/943)	RL	EU	05.07.2016	MS	▪ Erforderlich für den Schutz des GeschG ist unter anderem, dass die geheime Information zumindest einen potentiellen wirtschaftlichen Wert hat und Gegenstand angemessener Geheimhaltungsmaßnahmen ist. Deshalb sind vertragliche, organisatorische und/oder technische Vorkehrungen im Unternehmen erforderlich ▪ Als erlaubte Handlung ausdrücklich zulässig ist u.a. Reverse Engineering frei verfügbarer Produkte (§ 3 Abs. 1 Nr. 2 GeschGehG), das bisher in Deutschland eine rechtliche Grauzone bildete ▪ Gerechtfertigte Handlungen u.a. für Wistleblower und Journalisten (§ 5 GeschGehG)	▪ Ohne angemessene Geheimhaltungsmaßnahmen genießen Geschäftsgeheimnisse keinen Schutz ▪ Bei Zuwiderhandlung gegen Geheimhaltungspflichten im Prozess können Ordnungsgelder bis zu 100 000 Euro oder Ordnungshaft bis zu sechs Monaten festgesetzt werden			
Gesetz zum besseren Schutz von Geschäftsgeheimnissen(GeschGehG)	Umsetzung der Know-How-Schutz-RL	National	26.04.2019						UWG, aber GeschGehG lex specialis
Urheberrechtliche Schutz von Software gemäß UrhG		National	Letzte Novellierung 28.11.2019		▪ §§ 69a ff UrhG (Besondere Bestimmungen für Computerprogramme)				
Gesetz zur Digitalisierung der Energiewende		National	29.08.2016		▪ Anforderungen an Zertifizierung von Smart Meter Gateway / Zähler, basierend auf IT-Sicherheit und Datenschutz				

bitkom

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
Radio Equipment Directive (RED)	Aufnahme von Cyber-sicherheit geplant	EU	12. Juni 2014, fortlaufende Weiterent-wicklung	MS	▪ Art. 3 (3) der RE-D 2014/53/EU ermäch-tigt die Europäische Kommission sog. Delegierte Rechtsakte zu erlassen, die die Erfüllung von grundlegenden Anfor- derungen u.a. in Bezug auf den Schutz personenbezogener Daten, Betrug etc. zum Inhalt haben ▪ Aktivierung der Artikel 3 (3) d, e und f, sowie von Artikel 4 wird diskutiert ▪ Public Consultation on the upload of software into radio equipment – offen bis zum 14. September 2020 ▪ Targeted consultation on Reconfigurable Radio Systems (RRS) – bereits beendet ▪ Q3 2020 (early – July): Launching of a study in support of horizontal legislation (CNECT) ▪ Q4 2020: “Cybersecurity Strategy” ▪ Adoption of a delegated act on Article 3(3)(d?/e/f) of the RED ▪ First draft of the standardisation request available 1-2 months after adoption of the act ▪ Announcement and outline of the Horizontal regulation ▪ Q4 2020 / Jan 2021 Completion of the study on upload of software on radio equipment – Article 3(3)(i) and 4 of the RED ▪ Q4 2021: proposal for a Horizontal Regulation	Nicht konforme Produkte könnten vom Markt genom-men warden	V	BNetzA (BMWi) (Kontrolle durch Markt-überwachungs behörden)	EU Cybersecurity Act
Low Voltage Directive (LVD)	Anfang des Jahres gab es Stakeholder Survey und Public Consultation. Cybersicher-heit war nicht mit dabei	EU	Evaluation der LVD auf einen unbestimmten späteren Zeitpunkt 2020 verschoben bzw. Modifik-ation des Gesetzes-vorschlags	MS		Nicht konforme Produkte könnten vom Markt genom-men werden	V	BMAS (Kon-trolle durch Marktüberwa-chungsbehörden	EU Cybersecurity Act

bitkom

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
Machinery Directive (MD)	Bisher RL, soll VO werden Aufnahme von Cyber-sicherheit geplant	EU	17. Mai 2006 Revision der Maschinen-RL (Q4 2020): Novelle im Lichte neuer Technologien und als Verordnung in Q1 2021	MS	Verschiedene Optionen werden diskutiert: ▪ Keine Änderung ▪ Die Richtlinie an den NLF angleichen ▪ Anforderungen an Cybersicherheit aufnehmen ▪ Nicht an NLF angleichen, aber trotzdem neue Anforderungen wie Cybersicher-heit aufnehmen ▪ Unabhängig von den aufgezählten Opti-onen aus der Richtlinie eine Verordnung zu machen	Nicht konforme Produkte könnten vom Markt genom-men werden	V	BMAS (Kon-trolle durch Marktüberwa-chungsbehör-den)	
Digital Content Directive (DCD) & Sales of Goods Directive (SGD)	RL	EU	20.05.2019	MS	▪ Die DCD 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 SGD betrifft alle Warenverkäufe, unabhängig davon, ob sie physisch (in Geschäften), online oder im Fernabsatz erfolgen		V		
European Critical Infrastructure (ECI) Directive (2008/114/EG)	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 Weiterent-wicklung	Mobilitätssektor	▪ (Internationale) Harmonisierung der technischen Vorschriften für Kraftfahrzeuge ▪ Fragen rund um Automatisierung, Vernetzung und weitere Aspekte rund um die Mobilität der Zukunft			BMVI	
General Product Safety Directive (GPSD)	RL	EU	15.1.2002	MS	▪ Am 23. Juni 2020 wurde die Roadmap zur Überarbeitung der GPSD veröffentlicht ▪ Cybersicherheit soll aufgenommen werden				

bitkom