Regulierungsmapping IT-Sicherheit

Gesetzliche Anforderungen auf nationaler und europäischer Ebene

Stand: August 2019

bitkom

Herausgeber

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

Ansprechpartnerin

Teresa Ritter | Bereichsleiterin Sicherheitspolitik
T 030 27576-203 | t.ritter@bitkom.org

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 oder F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
					Kernthemen				
Telekommunikationsgesetz (TKG)	Z. T. Umsetzung europäischer Vorgaben	National	22.06.2004, seitdem zahlreiche Novellen	Betreiber von öffentlichen Telekommunikationsnetzen und die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten	Z. B. ▪ § 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 kommunikationsspezifischem Datenschutz
Telemediengesetz (TMG)	Z. T. Umsetzung europäischer Vorgaben, z. B. ePrivacy RL	National	26.02.2007, seitdem zahlreiche Novellen	Anbieter von Telemedien nach § 1 TMG			V	▪ Datenschutzaufsichtsbehörden ▪ An den Schnittstellen zum TKG: BNetzA ▪ Hinsichtlich Medien: Landesmedienanstalten	▪ ePrivacy Richtlinie (und zukünftig ePrivacy Verordnung) ▪ DS-GVO
NIS RL	Richtlinie	EU	29.06.2016	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	

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 oder F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
IT Sicherheitsgesetz (Artikelgesetz, Auswirkung auf: TKG, TMG, StGB, StPO, BSI-Gesetz)		Deutsche Umsetzung der NIS RL	30.06.2017, seit 10.05.2018 für Anbieter digitaler Dienste	Betreiber folgender wesentlicher Dienste: ▪ Finanzen und Versicherungen ▪ 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 (D)	Befindet sich in Ressortabstimmung		▪ Erweiterung der KRITIS um andere Branchen sowie Absenkung der Schwellenwerte, ▪ Freiwilliges IT-Sicherheitskennzeichen ▪ BSI bekommt Befugnisse beim Verbraucherschutz		V (KRITIS Erweiterung) und F (Zertifizierung & Gütesiegel)	BSI	Überlappung mit EU Cybersecurity Act
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 (European Network and Information Security Agency)	Keine Sanktionsmechanismen, da freiwillig	F	BSI / Enisa	Möglicherweise Überschneidung mit dem IT-Sicherheitsgesetz
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	
Datenschutzgrundverordnung (DS-GVO)	VO (+parallele RI für Polizei und Justiz)	EU	25.05.2018	MS	[...], Datensicherheit insb. Art. 32	Art. 83/84 DS-GVO	V	EDPB, nationale DPA	

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 oder F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
ePrivacy	VO	EU	Derzeit offen – Trilog wird sehr wahrscheinlich nicht mehr in dieser Legislatur stattfinden	MS	[…]	Wie DS-GVO	V	EDPB, nationale DPA	
1. und 2. DSAnpUG	Nationale Umsetzung DS-GVO	National	1. DSAnpUG: 25.05.2018 2. DSAnpUG: Voraussichtlich BR-Termin 14.12.2018, Inkrafttreten Anfang 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	
	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		
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 oder F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Vertrauensdienste-gesetz (VDG)	Nationales Gesetz	National	29.07.2017	Vertrauens-diensteanbieter in Deutschland	Anpassung alter Rechtslage (insb. Signaturgesetz) an eIDAS VO		V		
Vertrauensdienste-verordnung (VDV)	Nationales Gesetz	National	28.02.2019	Vertrauens-diensteanbieter in Deutschland	Anpassung alter Rechtslage (insb. Signaturverordnung) an eIDAS VO		V		
					Randthemen				
Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung	Richtlinie	EU	05.07.2016 (Veröffentlichung)	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) ▪ Gesetz gibt zudem Vorgaben für den Geheimnisschutz im Prozess ▪ S.o.	▪ 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-Richtlinie	National (D)	26.04.2019						UWG, aber GeschGehG lex specialis
Digital Content Directive (DCD) & Tangible Goods Directive (TGD)	Richtlinien	EU	Noch offen	MS	Updateverpflichtungen und Ausweitung des Gewährleistungsumfangs		V		

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 oder F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Radio Equipment Directive (RED)	Aufnahme von Cybersecurity geplant	EU	Verschiedene Delegated Acts geplant, Konsultationen dazu im Laufe dieses Jahres	MS	▪ Art. 3 (3) der RE-D 2014/53/EU ermächtigt die Europäische Kommission sog. Delegierte Rechtsakte zu erlassen, die die Erfüllung von grundlegenden Anforderungen u.a. in Bezug auf den Schutz personenbezogener Daten, Betrug etc. zum Inhalt haben ▪ Die Kommission hat vor kurzem eine roadmap für internetfähige- sowie tragbare Funkanlagen unter Art. 3 (3) veröffentlicht ▪ Von der Kommission ins Spiel gebrachte Optionen sind: 1. Wie bisher, keine Einführung von verpflichtenden Security Anforderungen 2. Selbstregulierung der Industrie 3. Delegated Act gemäß Art. 3 (3) lit. e) (Schutz personenbezogener Daten und der Privatsphäre) 4. Delegated Act gemäß Art. 3 (3) lit. f) (Schutz vor Betrug) 5. Delegated Act gemäß Art. 3 (3) lit. e) und f) ▪ Zeitplan der Kommission: ▪ Roadmap Feedback bis zum 25.2.2019 ▪ Öffentliche Konsultation in Q2/2019 ▪ Annahme des Delegierten Rechtsaktes durch die Kommission in Q4/2019	Nicht konforme Produkte könnten vom Markt genommen warden	V	BNetzA (BMWi) (Kontrolle durch Marktüberwachungsbehörden)	EU Cybersecurity Act
Low Voltage Directive (LVD)	Anfang des Jahres gab es Stakeholder Survey und Public Consultation und Cybersicherheit war nicht mit dabei	EU	Commission adoption Planned for Second quarter 2019	MS		Nicht konforme Produkte könnten vom Markt genommen warden	V	BMAS (Kontrolle durch Marktüberwachungsbehörden)	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 oder F)	Zuständige Behörden	Wechselwirkung zwischen den Gesetzen
Machinery Directive (MD)	Aufnahme von Cybersecurity geplant	EU	In Revision, Public Consultation bis 30 August 2019	MS	Verschiedene Optionen werden diskutiert: ▪ Keine Änderung ▪ Die Richtlinie an den NLF angleichen ▪ Die Richtlinie an den NLF angleichen und unter anderem Anforderungen an Cybersicherheit aufnehmen ▪ Nicht an NLF angleichen, aber trotzdem neue Anforderungen wie Cybersicherheit aufnehmen ▪ Unabhängig von den aufgezählten Optionen aus der Richtlinie eine Verordnung zu machen	Nicht konforme Produkte könnten vom Markt genommen warden	V	BMAS (Kontrolle durch Marktüberwachungsbehörden)	

bitkom