GRC+ DIGEST · 21 NOVEMBER 2026

Germany Digest

What applies in Germany, and by when. Each requirement with its dates, supervisors, incident deadlines and fines; then how GRC+ helps.

Coming Up

DATE	REQUIREMENT	WHAT HAPPENS
2 Dec 2026	AI Act	Marking of synthetic content, for systems already on the market
31 Dec 2026		Swift CSP attestation due
1 Jan 2027	DORA	Remaining KWG institutions outside DORA must apply DORA (section 1a(2a) KWG)
31 Jan 2027	NIS2 (BSIG)	Federal bodies report withheld information totals to the BSI

Three Requirements to Look at First

NATIONAL LAW UNDER NIS2 · IN FORCE

NIS2 (BSIG)

Key dates	**6 Dec 2025** In force, no transition period **31 Jan 2027** Federal bodies report withheld information totals to the BSI (coming up)
Incident reporting	Early warning: Without undue delay and in any event within 24 hours of becoming aware
Maximum fine	EUR 10 million or 2% of worldwide (group) annual turnover, whichever is higher (Particularly important)
Supervisors	BSI, CERT-Bund, BNetzA

NATIONAL LAW UNDER DORA · IN FORCE

DORA

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

EU REGULATION, APPLIES DIRECTLY · APPLIES IN STAGES

AI Act

Key dates	**2 Aug 2026** Transparency duties apply, the general date of application **2 Dec 2026** Marking of synthetic content, for systems already on the market (coming up)
Incident reporting	First notice: Within 2 days of becoming aware for a widespread infringement or critical infrastructure disruption; 10 days for a death; 15 days otherwise
Maximum fine	EUR 35 million or 7% of worldwide (group) annual turnover, whichever is higher (Article 99(3) prohibited practices)

The First Three in Detail

NATIONAL LAW UNDER NIS2 · IN FORCE

NIS2 (BSIG)

Rewrites the BSI Act: in-scope entities register with the BSI within three months, report incidents in 24 hours and answer through management.

Key dates	**6 Dec 2025** In force, no transition period **31 Jan 2027** Federal bodies report withheld information totals to the BSI (coming up) **11 Dec 2027** Remaining provisions of the German CRA implementing act take effect (coming up)
Supervisors	Federal Office for Information Security (BSI) Competent authority Federal CERT (CERT-Bund) CSIRT Federal Network Agency (BNetzA) Competent authority
Incident reporting	**Early warning** Without undue delay and in any event within 24 hours of becoming aware **Incident notification** Without undue delay and in any event within 72 hours of becoming aware (24 hours for trust service providers, for incidents affecting their trust services) **Intermediate report** On request **Final report** Within one month of the incident notification To: CSIRT or competent authority
Maximum fines	**Particularly important** EUR 10 million or 2% of worldwide (group) annual turnover, whichever is higher **Important** EUR 7 million or 1.4% of worldwide (group) annual turnover, whichever is higher
Managers	Managers can be held personally liable; Managers can be temporarily banned from their role
How we help	NIS2 Compliance Assessment Incident Reporting Desk

NATIONAL LAW UNDER DORA · IN FORCE

DORA

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

EU REGULATION, APPLIES DIRECTLY · APPLIES IN STAGES

AI Act

Sets risk-based requirements for AI providers and deployers in the EU, from banned practices to high-risk systems and general-purpose models.

Key dates	**2 Aug 2026** Transparency duties apply, the general date of application **2 Dec 2026** Marking of synthetic content, for systems already on the market (coming up) **2 Aug 2027** Existing general-purpose AI models must comply (coming up)
Incident reporting	**First notice** Within 2 days of becoming aware for a widespread infringement or critical infrastructure disruption; 10 days for a death; 15 days otherwise To: AI Office and, as appropriate, national competent authorities

Maximum fines	**Article 99(3) prohibited practices** EUR 35 million or 7% of worldwide (group) annual turnover, whichever is higher **Article 99(4) operator and notified body obligations** EUR 15 million or 3% of worldwide (group) annual turnover, whichever is higher **Article 99(5) incorrect, incomplete or misleading information** EUR 7.5 million or 1% of worldwide (group) annual turnover, whichever is higher **Article 101 general-purpose AI model providers (fined by the Commission)** EUR 15 million or 3% of worldwide (group) annual turnover, whichever is higher
How we help	EU AI Act Readiness Assessment

Every Other Requirement in Germany

The other requirements on the country page, with their status and the facts we have reviewed.

NATIONAL LAW UNDER GDPR · IN FORCE

GDPR (BDSG)

Applies the regulation in Germany, with federal and Land supervisors, a DPO duty where 20 or more people process data and employee data requirements.

Key dates	**25 May 2018** Entered into force
Supervisors	Federal Commissioner for Data Protection and Freedom of Information (BfDI) Data protection authority
Incident reporting	**Notification to the supervisory authority** Without undue delay and, where feasible, within 72 hours of becoming aware **Intermediate report** In phases, without undue further delay To: Competent supervisory authority
Maximum fines	**Article 83(4) infringements** EUR 10 million or 2% of worldwide (group) annual turnover, whichever is higher **Article 83(5) and (6) infringements** EUR 20 million or 4% of worldwide (group) annual turnover, whichever is higher The caps of GDPR apply.
How we help	Outsourced DPO Service Data Protection Compliance Audit

NATIONAL LAW UNDER CER · IN FORCE

CER (KRITIS-DachG)

Transposes the directive into German law, with the BBK as single point of contact and operators registering facilities on a BBK and BSI platform.

Key dates	**17 Mar 2026** Entered into force **29 Jul 2026** Act amending the KRITIS-DachG and BSIG registration requirements in force
Incident reporting	**First notice** Within 24 hours of becoming aware **Final report** Within one month of the initial notification, where relevant To: Competent authority
How we help	NIS2 Compliance Assessment Incident Reporting Desk

NATIONAL LAW UNDER EPRIVACY · IN FORCE

ePrivacy (TDDDG)

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

NATIONAL LAW UNDER PLD · ADOPTED, NOT YET IN FORCE

PLD (ProdHaftG)

Re-enacts the German Product Liability Act to cover software, AI systems and online platforms, keeping the development-risk defence.

Key dates	**8 Oct 2026** Adopted **9 Dec 2026** Enters into force (coming up)
How we help	Cyber Resilience Act Readiness Assessment

NATIONAL LAW UNDER PSD2 · IN FORCE

PSD2 (ZAG)

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

NATIONAL LAW · IN FORCE

EnWG

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

NATIONAL LAW · IN FORCE

MaRisk

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

NATIONAL LAW · IN FORCE

TKG

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

NATIONAL LAW · IN FORCE

§ 393 SGB V

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

NATIONAL LAW · IN FORCE

§§ 390–392 SGB V

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

EU REGULATION, APPLIES DIRECTLY · APPLIES IN STAGES

AI Omnibus

Amends the AI Act to postpone high-risk obligations, extend SME relief to small mid-caps and add bans on AI-generated intimate and abuse imagery.

Key dates	**27 Jul 2026** Enters into force **2 Dec 2026** New prohibitions apply (coming up) **2 Dec 2027** High-risk requirements for Annex III systems apply (coming up)
How we help	EU AI Act Readiness Assessment

EU REGULATION, APPLIES DIRECTLY · IN FORCE SINCE 10 DECEMBER 2024

CRA

Sets cybersecurity requirements for hardware and software products sold in the EU, with vulnerability reporting and CE marking for manufacturers.

Key dates	**11 Sep 2026** Reporting obligations apply **11 Dec 2027** All obligations apply (coming up) **11 Jun 2028** Last day earlier type-examination certificates stay valid (coming up)
Incident reporting	**First notice** Within 24 hours of becoming aware **Incident notification** Within 72 hours of becoming aware **Intermediate report** On request of the coordinating CSIRT **Final report** Within one month of the incident notification To: Coordinating CSIRT and ENISA, via the single reporting platform
Maximum fines	**Article 64(2) essential requirements and Articles 13 and 14** EUR 15 million or 2.5% of worldwide (group) annual turnover, whichever is higher **Article 64(3) other listed obligations** EUR 10 million or 2% of worldwide (group) annual turnover, whichever is higher **Article 64(4) incorrect, incomplete or misleading information** EUR 5 million or 1% of worldwide (group) annual turnover, whichever is higher
How we help	Cyber Resilience Act Readiness Assessment

EU REGULATION, APPLIES DIRECTLY · IN FORCE SINCE 4 FEBRUARY 2025

Cyber Solidarity Act

Builds EU capacity to detect and respond to large-scale cyber incidents through cyber hubs, an emergency mechanism and a cybersecurity reserve.

Key dates	**15 Jan 2025** Published in the Official Journal **4 Feb 2025** Enters into force and applies
How we help	Incident Response Plan and Exercise

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 27 JUNE 2019

Cybersecurity Act

Gives ENISA a permanent mandate and sets up the EU certification framework for ICT products, services and processes, starting with EUCC.

Key dates	**27 Jun 2019** In force **27 Feb 2025** EUCC scheme applies

Supervisors	European Union Agency for Cybersecurity (ENISA) Competent authority
How we help	Penetration Testing

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 12 SEPTEMBER 2025

Data Act

Gives users of connected products the right to access and share the data they generate, and makes switching cloud providers easier.

Key dates	**12 Sep 2025** Requirements apply **12 Jan 2027** Switching charges abolished (coming up) **12 Sep 2027** Chapter IV reaches older long-term contracts (coming up)
Maximum fines	**Article 40(4): Chapters II, III and V, fines by data protection authorities within their competence; all other fines are set nationally** EUR 20 million or 4% of worldwide (group) annual turnover, whichever is higher
How we help	Outsourced DPO Service

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 24 SEPTEMBER 2023

DGA

Sets requirements for re-using protected public sector data, for data intermediation services and for data altruism organisations in the EU.

Key dates	**23 Jun 2022** Enters into force **24 Sep 2023** Requirements apply **24 Sep 2025** Transitional period ends for intermediation services provided on 23 June 2022
How we help	Outsourced DPO Service

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 2 MAY 2023

DMA

Sets conduct requirements for designated gatekeeper platforms so digital markets stay open to competitors and fair to business users and consumers.

Key dates	**2 May 2023** Requirements apply
Supervisors	European Commission Competent authority
How we help	Government Relations as-a-Service

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 17 FEBRUARY 2024

DSA

Sets requirements for online intermediaries in the EU on illegal content, user transparency and, for the largest platforms, systemic risk management.

Key dates	**25 Aug 2023** Obligations apply to the first very large platforms and search engines **17 Feb 2024** Applies to all providers
Supervisors	European Commission Competent authority Federal Network Agency (BNetzA) Competent authority

How we help DSA Compliance Review

EU REGULATION, APPLIES DIRECTLY · APPLIES IN STAGES

EHDS

Gives people access to their electronic health data across the EU, sets requirements for EHR systems and governs secondary use of health data.

Key dates **11 Oct 2026** Dataset metadata implementing regulation (EU) 2026/2098 in force
26 Mar 2027 EHDS applies, apart from the provisions phased in from 2029 (coming up)
26 Mar 2029 Priority categories, EHR systems and most secondary use requirements apply (coming up)

How we help Outsourced DPO Service

EU REGULATION, APPLIES DIRECTLY · APPLIES IN STAGES

eIDAS 2

Requires each Member State to offer digital identity wallets that banks and large platforms must accept, and adds new qualified trust services.

Key dates **20 May 2024** In force
23 Feb 2027 Reference formats for advanced signatures and seals apply (coming up)
17 May 2027 Transitional accreditation of trust service assessment bodies ends (coming up)

How we help CISO as-a-Service

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 26 MAY 2021

MDR

Sets safety and performance requirements for medical devices and software on the EU market, including protection against unauthorised access.

Key dates **26 May 2021** Requirements apply
31 Dec 2027 End of transition for class III and implantable class IIb legacy devices (coming up)
31 Dec 2028 End of transition for other legacy devices (coming up)

How we help CISO as-a-Service

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 30 DECEMBER 2024

MiCA

Requires crypto-asset issuers and service providers in the EU to obtain authorisation, publish white papers and meet conduct requirements.

Key dates **30 Dec 2024** Requirements apply
1 Jul 2026 Transitional period for crypto-asset service providers ends at the latest
31 Dec 2027 Trading platforms ensure white papers for crypto-assets admitted to trading before 30 December 2024 (coming up)

How we help MiCA Compliance Audit

EU REGULATION, APPLIES DIRECTLY · APPLIES IN STAGES

NCCS

Requires high-impact and critical-impact electricity entities to assess cyber risk, apply minimum or advanced controls and manage supply chain risk.

Key dates	**13 Jun 2024** Enters into force
How we help	IEC 62443 Security Assessment

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 22 FEBRUARY 2026

Part-IS

Requires aviation organisations and authorities to run an information security management system and report incidents that could affect safety.

Key dates	**16 Oct 2025** Regulation (EU) 2022/1645 applies **22 Feb 2026** Regulation (EU) 2023/203 applies
Supervisors	European Union Aviation Safety Agency (EASA) Competent authority Federal Aviation Office (LBA) Competent authority
How we help	ISO 27001 Implementation

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 1 AUGUST 2025

RED DA

Requires internet-connected radio equipment, toys and wearables to protect networks and personal data and to guard against fraud.

Key dates	**1 Feb 2022** Enters into force **1 Aug 2025** Requirements apply
How we help	Penetration Testing

EU REGULATION, APPLIES DIRECTLY · APPLIES SINCE 7 JULY 2024

UN R155 / R156

Makes certified cyber security and software update management systems a condition of type approval for new cars, vans, buses and trucks.

Key dates	**6 Jul 2022** EU: mandatory for new vehicle types **7 Jul 2024** EU: mandatory for all newly registered vehicles
How we help	CISO as-a-Service

STANDARD · IN FORCE

BSI C5

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · APPLIES SINCE 1 FEBRUARY 2023

IT-Grundschutz

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · IN FORCE

IT-Sicherheitskatalog

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · IN FORCE

TIBER-DE

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · IN FORCE

TISAX

Assesses automotive suppliers and service providers against the VDA ISA catalogue through accredited auditors, with results shared with customers.

Key dates	**1 Apr 2024** ISA 6 Applies **1 Jan 2027** VDA ISA2027 Applies (coming up)
How we help	ISO 27001 Implementation

Requirements by Sector

SECTOR	REQUIREMENTS	STANDARDS	SUPERVISORS
Automotive and Transportation	UN R155 / R156, Data Act, NIS2 (BSIG), CER (KRITIS-DachG)	TISAX, ISO/SAE 21434, ISO 24089, ISO 27001, NIST CSF	BSI, BNetzA
Financial Services and Insurance	DORA, MaRisk, PSD2 (ZAG), MiCA, §§ 390–392 SGB V, eIDAS 2, GDPR (BDSG), NIS2 (BSIG)	TIBER-DE, Swift CSP, PCI DSS, HITRUST, ISO 27799	BaFin, Deutsche Bundesbank, EBA, ECB, EIOPA, ESMA
Energy and Utilities	EnWG, NCCS, NIS2 (BSIG), CER (KRITIS-DachG)	IT-Sicherheitskatalog, IEC 62443, ISO 27001, IEC 62351, ISO/IEC 27019	BNetzA, BSI
Healthcare and Life Sciences	EHDS, MDR, PLD (ProdHaftG), § 393 SGB V, §§ 390–392 SGB V, GDPR (BDSG), CER (KRITIS-DachG)	BSI C5, HITRUST, ISO 27799, SOC 2, IEC 80001-1	BSI, BfArM, PEI
Technology and Telecom	TKG, ePrivacy (TDDDG), § 393 SGB V, CRA, DMA, DSA, Data Act, eIDAS 2	BSI C5, GSMA NESAS, ISO 22301, AIUC-1, ISO/IEC 27017	BNetzA, BfDI, BSI
Public Sector and Defence	DGA, eIDAS 2, GDPR (BDSG), NIS2 (BSIG), CER (KRITIS-DachG)	IT-Grundschutz, BSI C5, COBIT, ISO 27001, ISO/IEC 27701	BSI, CERT-Bund, BfDI

Retail, Consumer and Leisure	ePrivacy (TDDDG), DMA, DSA, eIDAS 2, GDPR (BDSG), CER (KRITIS-DachG)	PCI DSS, ETSI EN 303 645, ISO/IEC 27701, NIST Privacy Framework, CIS Controls	BSI
Aviation and Space	Part-IS, CER (KRITIS-DachG)	ISO 27001, ED-202A / DO-326A, ISO 9001, ISO 31000, ISO/IEC 27005	LBA, BSI, EASA
Manufacturing and Chemicals	RED DA, PLD (ProdHaftG), CRA, Data Act, NIS2 (BSIG)	IEC 62443, ISO 27001, NIST CSF, CLC/TS 50701, ETSI EN 303 645	

Who Supervises

SUPERVISOR	SUPERVISES	WEBSITE
Federal Aviation Office LBA	Part-IS	lba.de
Federal CERT CERT-Bund	NIS2 (BSIG)	bsi.bund.de
Federal Commissioner for Data Protection and Freedom of Information BfDI	GDPR (BDSG)	bfdi.bund.de
Federal Network Agency BNetzA	NIS2 (BSIG), DSA	bundesnetzagentur.de
Federal Office for Information Security BSI	NIS2 (BSIG)	bsi.bund.de
European Commission EU level	DMA, DSA	commission.europa.eu
European Union Agency for Cybersecurity ENISA EU level	Cybersecurity Act	enisa.europa.eu
European Union Aviation Safety Agency EASA EU level	Part-IS	easa.europa.eu

How GRC+ Helps

We never audit work our own team runs for you. A team of four to five practitioners, under one contract for every country you operate in.

Stay Compliant Ongoing work: pay as you go or monthly.	Incident Reporting Desk Vendor Risk Management EU and UK Representative CISO as-a-Service Outsourced DPO Service AI Governance Officer as-a-Service Compliance Officer as-a-Service Internal Audit as-a-Service Government Relations as-a-Service

Audit or Assess An independent view, because a regulation requires one or because you want to know for yourself. We never audit a role our own team runs for you.	Swift CSP Assessment ISO 27001 Internal Audit NIS2 Compliance Assessment DORA Compliance Audit Data Protection Compliance Audit PCI DSS Readiness Assessment EU AI Act Readiness Assessment SOC 2 and Assurance Report Review DSA Compliance Review IEC 62443 Security Assessment MiCA Compliance Audit Security Maturity Assessment Post-Quantum Cryptography Readiness Assessment PSD2 SCA Audit Security Architecture Review Cyber Resilience Act Readiness Assessment ISO 42001 Internal Audit ISO 27701 Internal Audit Data Protection Impact Assessment (DPIA)
Build and Fix One-off work that closes the gaps.	NIS2 Readiness Programme DORA Gap Remediation AI Act Compliance Programme ISO 27001 Implementation Incident Response Plan and Exercise
Security Testing Tests that show whether attacks are detected and stopped.	Red Teaming Penetration Testing Cloud Security Assessment Source Code Review

Talk to Us

Thirty minutes with a principal consultant on what applies to you and what to do first.

Book a 30-Minute Call · sales@grc.plus · +31 20 241 66 00

Dates and requirements come from the GRC+ regulation pages and change as they do. The latest version: grc.plus/de