NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 6/2026

Levent Ferik

EDITORIAL

Bettina Gayk, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW), bringt es bei der Vorstellung ihres 31. Tätigkeitsberichts auf den Punkt: „Datennutzung ist in aller Munde und das neue Synonym für Fortschritt. Ich möchte aber davor warnen, die Gefahren ungezügelter Datennutzung zu ignorieren."

Die Zahlen stützen diese Einschätzung. 12.592 Datenschutzbeschwerden gingen im Jahr 2025 bei der LDI NRW ein. Das ist ein Anstieg von mehr als 67 Prozent gegenüber dem Vorjahr. Die verhängten Geldbußen näherten sich zudem der Marke von einer halben Million Euro. Was steckt dahinter? Der Bericht zeigt ein vertrautes Muster: Medizinisches Personal veröffentlicht Patientendaten in sozialen Medien. Ein Reiseveranstalter nutzt Urlaubsvideos von Gästen ohne deren Einwilligung zu Werbezwecken. Ein Taxiunternehmen gibt Gesundheitsdaten von Fahrgästen über WhatsApp weiter. Und ein Telekommunikationsanbieter missachtet systematisch Auskunftsrechte – mit einer empfindlichen Geldbuße als Folge.

Besonderes Gewicht hat in dem Bericht die Kritik an zwei neuen NRW-Sicherheitsgesetzen. Sowohl das überarbeitete Polizeigesetz (PolG) als auch das neue Verfassungsschutzgesetz erlauben den Behörden den Einsatz von künstlicher Intelligenz (KI) – nach Gayks Einschätzung jedoch zu pauschal und ohne ausreichende Differenzierung. Wer KI nutzt, um Texte verständlicher zu formulieren, brauche dafür keine Sonderbefugnis. Wer hingegen mithilfe von KI Anhaltspunkte für verfassungsfeindliche Tendenzen ermittelt, greife potenziell tief in die Privatsphäre aller Bürgerinnen und Bürger ein – mit Fehlerrisiken, die nicht kleinzureden sind.

Der Bericht ist eine nüchterne Bestandsaufnahme eines Jahres, in dem der Datenschutz an vielen Stellen unter Druck geraten ist. Lesenswert – nicht nur für Datenschutzbeauftragte.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

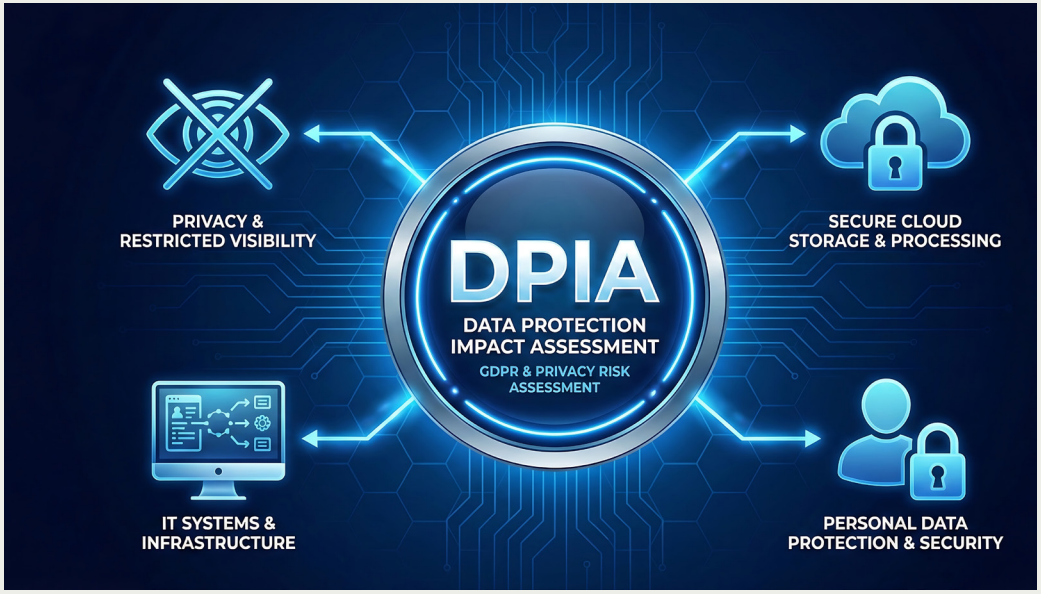


Foto: Onetrick , Adobe Stock

Einheitliches DSFA-Muster veröffentlicht

Der Europäische Datenschutzausschuss (EDSA) hat am 10. März 2026 ein standardisiertes Muster für Datenschutz-Folgenabschätzungen (DSFA/DPIA) nach Art. 35 Datenschutz-Grundverordnung (DS-GVO) verabschiedet und am 14. April 2026 zur öffentlichen Konsultation gestellt. Rückmeldungen können bis zum 9. Juni 2026 eingereicht werden. Ziel ist eine europaweit einheitliche DSFA-Dokumentation: Nach Abschluss der Konsultation sollen alle nationalen Datenschutzbehörden das Template als gemeinsames Muster oder zumindest als kompatibles „Meta-Template" übernehmen.

Aufbau und Struktur

Das Template gliedert sich in sechs inhaltliche Abschnitte, die aufeinander aufbauen und gezielt Querverweise ermöglichen sollen. Es beginnt mit einer Übersicht zur Verarbeitung, einschließlich Angaben zu Verantwortlichem, Auftragsverarbeitern, Bezeichnung und Planungszeitraum, und führt über eine systematische Beschreibung der Verarbeitung (Datenkategorien, Zwecke, Verarbeitungsumfang und -kontext, technische Infrastruktur) zur Compliance-Analyse. Diese umfasst die Prüfung der Rechtsgrundlagen, die Datenminimierung, die Speicherfristen sowie Maßnahmen zur Umsetzung von Betroffenenrechten, den Datenschutz durch Technikgestaltung (Art. 25 DS-GVO) und die Datensicherheit (Art. 32 DS-GVO).

Risikobetrachtung in zwei Dimensionen

Besonders strukturiert ist die Risikoanalyse: Das Template unterscheidet systematisch zwischen Risiken, die sich aus dem bestimmungsgemäßen Betrieb der Verarbeitung ergeben – also durch die Verarbeitungsstruktur selbst –, und solchen, die durch unbeabsichtigte, rechtswidrige oder anormale Ereignisse wie Cyberangriffe, Fehlkonfigurationen oder Insidermissbrauch entstehen. Für beide Dimensionen sind die Eintrittswahrscheinlichkeit, die Schwere und risikobeeinflussende Faktoren zu bewerten. Dem schließt sich ein Aktionsplan mit zusätzlichen Abhilfemaßnahmen und einer Restrisikobewertung an.

Einbindung von DSB und Betroffenen

Das Template sieht explizit vor, die Stellungnahme des Datenschutzbeauftragten (DSB) sowie gegebenenfalls die Perspektive betroffener Personen oder ihrer Vertreter zu dokumentieren. Den Abschluss bildet eine formale Entscheidung über die Durchführbarkeit der Verarbeitung – von der Aufgabe über die vorherige Konsultation der Aufsichtsbehörde bis hin zur bedingten oder uneingeschränkten Freigabe.
Verantwortliche werden ausdrücklich ermutigt, das Template bereits jetzt in der Praxis zu erproben und Feedback im Rahmen der laufenden Konsultation einzureichen.

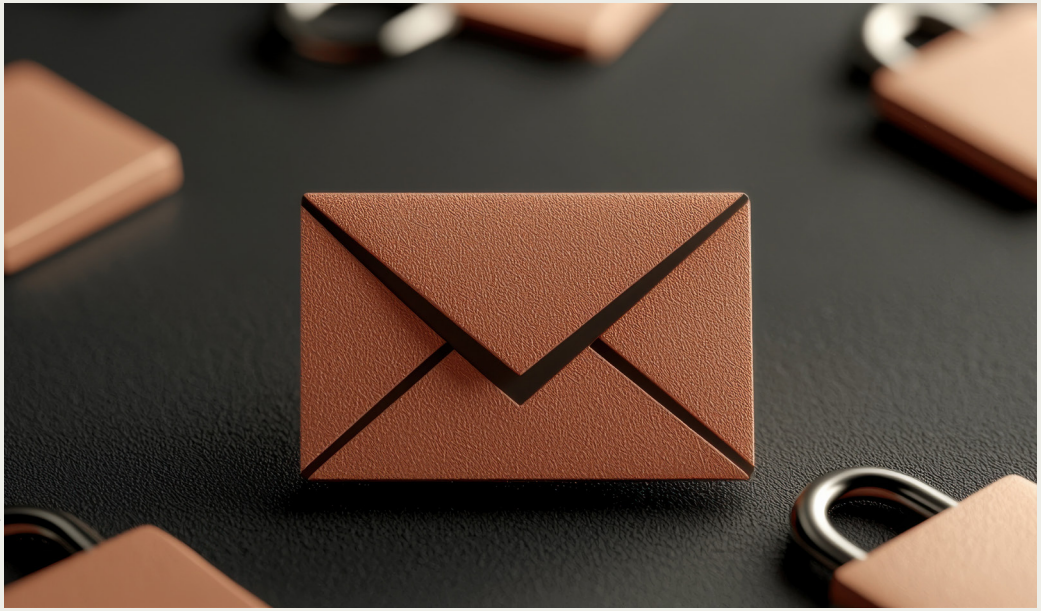


Foto: ParinApril, Adobe Stock

Anforderungen an die E-Mail-Sicherheit nach Art. 32 DS-GVO

Mit Urteil vom 2. April 2026 (Az. 29 K 7351/23) hat das Verwaltungsgericht Düsseldorf entschieden, dass die Übermittlung personenbezogener Daten per E-Mail mittels Transportverschlüsselung grundsätzlich ein dem Risiko angemessenes Schutzniveau im Sinne von Art. 32 DS-GVO gewährleistet. Eine Ende-zu-Ende-Verschlüsselung ist nicht generell erforderlich.

Sachverhalt

Dem Verfahren lag ein Verkehrsunfall zugrunde, bei dem ein Busunternehmen den Namen des Betroffenen, für den eine Melderegisterauskunftssperre nach § 51 Bundesmeldegesetz (BMG) bestand, per E-Mail an seine Kfz-Haftpflichtversicherung übermittelte. Der Kläger sah darin einen Verstoß gegen Art. 32 DS-GVO und begehrte von der LDI NRW als Aufsichtsbehörde aufsichtsrechtliche Maßnahmen, darunter die Anordnung einer verpflichtenden Ende-zu-Ende-Verschlüsselung sowie die Verhängung eines Bußgeldes.

Kernaussage zum Schutzniveau

Das Gericht bestätigte, dass Art. 32 DS-GVO keine absolut höchstmögliche Sicherheit verlangt, sondern eine risikoproportionale Schutzmaßnahme. Im konkreten Fall waren lediglich der Name und der Vorname des Klägers übermittelt worden – Daten, die nicht als sensibel einzustufen und im Internet frei zugänglich sind. Ein Bezug zur geschützten Privatanschrift war nicht herstellbar. Die Auskunftssperre im Melderegister begründet nach Auffassung des Gerichts kein erhöhtes Risiko, das über die Transportverschlüsselung hinausgehende Maßnahmen erfordern würde. Eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO war mangels hohen Risikos ebenfalls nicht geboten.

Verspätete Auskunft: teilweise Klagestattgabe

Einen Teilerfolg erzielte der Kläger in Bezug auf die Auskunftspflicht nach Art. 15 DS-GVO. Das Unternehmen hatte auf den Auskunftsantrag vom April 2022 erst im Oktober 2022 reagiert und damit die Monatsfrist des Art. 12 Abs. 3 DS-GVO deutlich überschritten. Das Gericht verpflichtete die LDI NRW zur Neubescheidung der Beschwerde in diesem Punkt, da die Aufsichtsbehörde den Verstoß im ursprünglichen Bescheid nicht als solchen erkannt und ihr Auswahlermessen hinsichtlich möglicher Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO nicht ausgeübt hatte. Ein Anspruch auf Verhängung eines Bußgeldes bestand mangels Ermessensreduzierung auf null nicht.

Das Urteil liefert praxisrelevante Orientierung für die Beurteilung technischer Schutzmaßnahmen bei der E-Mail-Kommunikation. Zugleich verdeutlicht es, dass Aufsichtsbehörden Beschwerden zu Auskunftsverstößen sorgfältig auf ihren Ermessensspielraum hin prüfen müssen.

Verzeichnis von Verarbeitungstätigkeiten

Erlernen Sie den Aufbau und die Pflege des Verzeichnisses von Verarbeitungstätigkeiten gemäß DS-GVO.

9. Juli 2026 | Online | 10.00-17.00 Uhr
Referent: Peter Schiefer

Schwerpunkte:

- ✓ Erklärung der Begriffe und Basiserfordernisse
- ✓ Organisieren und Priorisieren der Arbeitsschritte
- ✓ Identifizieren, Priorisieren und Beschreiben einzelner Verarbeitungstätigkeiten
- ✓ Praktische Umsetzung der Verarbeitungsprüfung
- ✓ Wichtige Aspekte in Bezug auf die Rechenschaftspflichten

Jetzt anmelden: **www.datakontext.com**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: Olivier Le Moal, Adobe Stock

Werbliche Nutzung von Kundendaten: Wie lange ist zu lange?

Eine einmalige Kundenbeziehung, die neun Jahre zurückliegt – reicht das als Grundlage für postalische Direktwerbung? Mit dieser Frage hat sich der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) in seinem 54. Tätigkeitsbericht (Ziffer 11.3) befasst und dabei grundlegende Maßstäbe für die zeitliche Zulässigkeit werblicher Datenverarbeitung herausgearbeitet.

Rechtsgrundlage und Einzelfallbetrachtung

Anders als beim E-Mail-Marketing, das grundsätzlich eine vorherige Einwilligung erfordert, kann postalische Direktwerbung auf Art. 6 Abs. 1 lit. f DS-GVO, das berechtigte Interesse, gestützt werden. Erwägungsgrund 47 DS-GVO bestätigt dies ausdrücklich. Eine abstrakte gesetzliche Speicherfrist für Werbedaten existiert jedoch nicht. Die DSK-Orientierungshilfe zur Direktwerbung (2022) verweist stattdessen auf eine Einzelfallbetrachtung, bei der insbesondere der zeitliche Abstand seit dem letzten aktiven Kontakt und die Art des zugrunde liegenden Geschäfts zu berücksichtigen sind.

Der konkrete Fall: Produktlebensdauer als Argument

Das betroffene Unternehmen hatte die werbliche Ansprache inaktiver Kund*innen schrittweise auf den Postweg reduziert und die Kontaktfrequenz verringert – eine für sich genommen nachvollziehbare Vorgehensweise. Als Abwägungsargument für die lange Speicherdauer verwies es auf die hohe Qualität und Langlebigkeit seiner Produkte, aus der sich ein verzögerter Wiederbeschaffungsbedarf ergebe. Der HBDI hält ein solches produktbezogenes Argument im Rahmen der Interessenabwägung grundsätzlich für berücksichtigungsfähig.

Entscheidend: Die dreijährige Unterbrechung

Was den Fall letztlich kippen ließ, war eine dreijährige vollständige Aussetzung der werblichen Datenverarbeitung, nach der das Unternehmen im neunten Jahr nach dem einzigen Einkauf die Ansprache wieder aufnahm. Diese Unterbrechung begründete bei der Betroffenen die berechtigte Erwartung, dass ihre Daten nicht mehr aktiv genutzt würden. Der HBDI wertete die Wiederaufnahme als nicht mehr verhältnismäßig: Wer nur einmalig Kunde war, muss vernünftigerweise nicht damit rechnen, dass seine Daten nach einem derart langen Zeitraum noch für Werbezwecke reaktiviert werden. Das Unternehmen präzisierte im Nachgang seine internen Richtlinien zu Speicherfristen und werblicher Kontaktaufnahme.

Foto: studio v-zwoelf, Adobe Stock

Niederlegung des DSB-Mandats: Was gibt es zu beachten?

Weder die DS-GVO noch das Bundesdatenschutzgesetz (BDSG) regeln ausdrücklich, wie ein Datenschutzbeauftragter (DSB) sein Amt aus eigener Initiative beenden kann. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) hat sich in seinem 54. Tätigkeitsbericht (Ziffer 8.2 ⭳) mit dieser praxisrelevanten Frage befasst und gibt differenzierte Orientierung – gestützt auf die einschlägige Kommentarliteratur.

Grundsatz: Amtsniederlegung ist möglich

Ungeachtet der fehlenden gesetzlichen Regelung geht die Kommentarliteratur einhellig davon aus, dass sowohl interne als auch externe Datenschutzbeauftragte (bei öffentlichen wie nicht-öffentlichen Stellen) ihr Amt niederlegen können. Eine Begründung dafür ist grundsätzlich nicht erforderlich. Entscheidend ist jedoch, dass dem Verantwortlichen ausreichend Zeit für die Benennung einer Nachfolge eingeräumt wird. Wird diese Übergangsfrist nicht gewahrt, kann eine Schadensersatzpflicht gegenüber dem Verantwortlichen entstehen.

Interne DSBs: arbeits- und dienstrechtliche Dimension

Interne DSBs erklären die Niederlegung gegenüber dem Verantwortlichen – aus Nachweisbarkeitsgründen – schriftlich mit nachweisbarem Zugang. Neben der datenschutzrechtlichen Dimension sind arbeits- bzw. dienstrechtliche Aspekte zu berücksichtigen: Bei Beamten erfolgt die Benennung regelmäßig im Wege des Direktionsrechts, bei Arbeitnehmer*innen durch entsprechende Vertragsanpassungen. Legt ein interner DSB einer nicht-öffentlichen Stelle sein Amt aus wichtigem Grund im Sinne des § 626 BGB nieder, muss dieser Grund dem Verantwortlichen gegenüber benannt werden. Zudem greift in diesem Fall der Kündigungsschutz nach § 6 Abs. 4 Satz 3 BDSG. Bei öffentlichen Stellen ist zu beachten, dass ein stellvertretender DSB benannt sein muss. Dessen Vorhandensein ist bei der Berechnung der Niederlegungsfrist zu berücksichtigen.

Externe DSBs: Vertragsrecht entscheidet

Für externe DSBs richtet sich die Amtsbeendigung nach dem zugrunde liegenden Dienstleistungsvertrag. Die dort vereinbarten Kündigungsmodalitäten – Form, Frist, Adressat – sind verbindlich einzuhalten. In der Regel ist eine schriftliche, fristgerechte Kündigung gegenüber dem Verantwortlichen erforderlich.

Foto: hathairat, Adobe Stock

Einheitliches Meldeformular für Datenpannen

Wer als Verantwortlicher oder externer Datenschutzdienstleister eine Datenpanne an mehrere Aufsichtsbehörden melden muss, sieht sich derzeit mit einem erheblichen bürokratischen Aufwand konfrontiert: Jede Behörde stellt ein eigenes Meldeformular bereit – und das unter dem engen Zeitdruck der 72-Stunden-Frist nach Art. 33 DS-GVO. Diesem strukturellen Problem widmen sich sowohl die Datenschutzkonferenz (DSK) als auch der Europäische Datenschutzausschuss (EDSA) mit konkreten Vereinheitlichungsplänen.

Wer besonders betroffen ist

Den größten Aufwand haben Unternehmen ohne EU-Niederlassung, zentrale Datenschutzabteilungen in Konzernen sowie externe Datenschutzberater*innen, die Meldungen für Verantwortliche in verschiedenen Bundesländern oder Mitgliedstaaten übernehmen. Besonders bei Cyberangriffen auf IT-Dienstleister, die für mehrere Auftraggeber tätig sind, muss derselbe Sachverhalt vielfach parallel an unterschiedliche Stellen gemeldet werden.

Stand der Initiativen

Die DSK hatte das Thema bereits in einer Arbeitsgruppe aufgegriffen. Der EDSA schloss sich mit seiner Helsinki-Erklärung vom Juli 2025 an und nahm die Umsetzung eines gemeinsamen Meldeformulars in sein Arbeitsprogramm 2026–2027 auf. Die LDI NRW, bei der im Jahr 2025 insgesamt 2.844 Datenpannenmeldungen eingingen, begleitet den Prozess aktiv, mit dem Ziel, dass die Vereinheitlichung weder bei Behörden noch bei meldenden Stellen zu Mehraufwänden führt.

Europäische Kommission denkt weiter

Noch einen Schritt weiter geht ein Vorschlag der Europäischen Kommission: Ein zentraler „Single Entry Point" bei der EU-Cybersicherheitsbehörde ENISA soll künftig ermöglichen, mit einer einzigen Meldung mehrere parallele Meldepflichten (DS-GVO, NIS-2, DORA, CER und eIDAS) gleichzeitig zu erfüllen. Davon würden insbesondere regulierte Finanzunternehmen profitieren, die bei IT-Sicherheitsvorfällen regelmäßig unter mehreren Regelwerken gleichzeitig meldepflichtig sind. Ob und wann diese zentrale Stelle tatsächlich eingerichtet wird, ist allerdings noch offen.

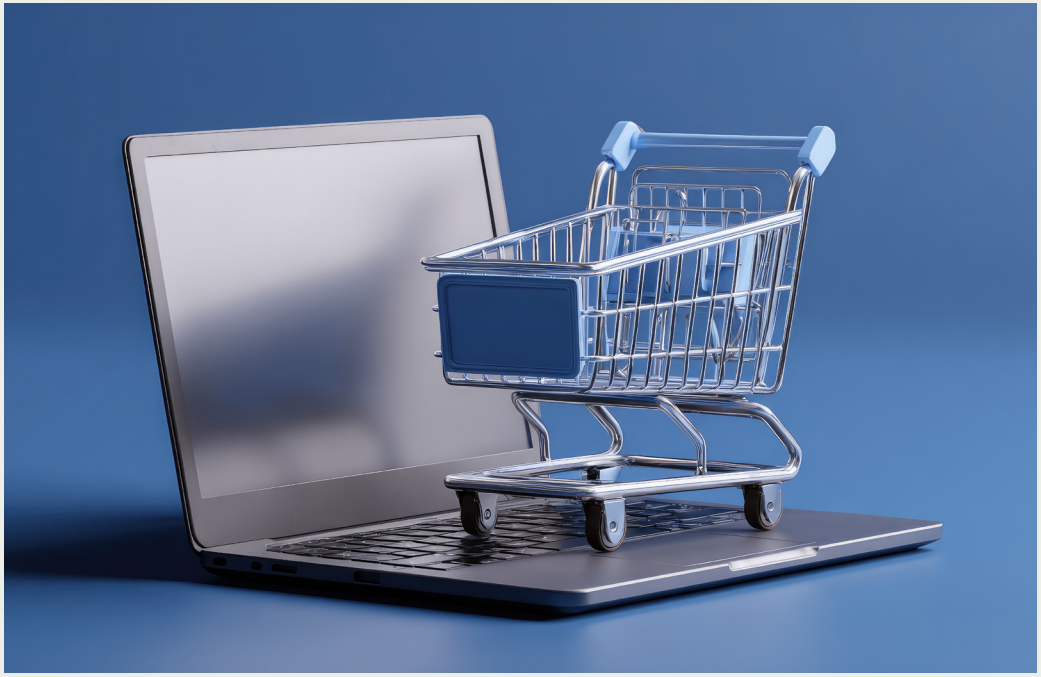


Foto: amai line art, Adobe Stock

Datenschutzkonforme Umsetzung von Warenkorb-Erinnerungsmails

Darf ein Onlinehändler Kund*innen per E-Mail an einen abgebrochenen Bestellvorgang erinnern? Mit dieser Frage hat sich die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) befasst und dabei eine klare rechtliche Einordnung vorgenommen, die für datenschutzrechtlich Verantwortliche im E-Commerce von erheblicher praktischer Relevanz ist.

Kein Vertrag, keine Rechtsgrundlage nach Art. 6 Abs. 1 lit. b DS-GVO

Auslöser war die Beschwerde eines Nutzers, der nach einem Kaufabbruch drei Erinnerungs-Mails erhalten hatte. Der Händler qualifizierte dies als zulässige „Servicekommunikation" – eine Einschätzung, die die LDI NRW nicht teilte. Das Verlassen eines Online-Shops ohne Kaufabschluss beendet das vorvertragliche Verhältnis; eine Rechtsgrundlage nach Art. 6 Abs. 1 lit. b DS-GVO scheidet damit aus.

Warenkorb-Erinnerungen sind Direktwerbung

Entscheidend für die Bewertung ist die rechtliche Einordnung solcher E-Mails als Direktwerbung im Sinne des Wettbewerbsrechts. Da sie auf ein zuvor beobachtetes Kaufverhalten abzielen und der Umsatzsteigerung dienen, handelt es sich um Retargeting und nicht um neutrale Servicekommunikation. Damit greifen sowohl § 7 Abs. 2 Nr. 1 Gesetz gegen den unlauteren Wettbewerb (UWG) als auch die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO: Die Interessen der betroffenen Personen an unverlangt zugesandter Werbung überwiegen grundsätzlich die Werbeinteressen der Verantwortlichen. Ohne ausdrückliche Einwilligung, etwa per Checkbox mit Double-Opt-in, ist die Verarbeitung unzulässig.

Ausnahme für Bestandskund*innen

§ 7 Abs. 3 UWG erlaubt Warenkorb-Erinnerungen unter engen Voraussetzungen auch ohne Einwilligung, sofern die E-Mail-Adresse im Rahmen eines bereits abgeschlossenen Kaufvertrags erlangt wurde, die Werbung ähnliche Waren oder Dienstleistungen betrifft, kein Widerspruch vorliegt und auf das jederzeitige Widerspruchsrecht hingewiesen wurde. Im konkreten Beschwerdefall griff diese Ausnahme jedoch nicht, da mangels abgeschlossener Erstbestellung keine Bestandskundenbeziehung bestand. Die LDI NRW empfiehlt Onlinehändler*innen, bei der Erhebung von E-Mail-Adressen transparent über den vorgesehenen Verwendungszweck zu informieren und Einwilligungen datenschutzkonform einzuholen.

Verhaltensregeln der deutschen Versicherungswirtschaft genehmigt

Die Versicherungsbranche erhält erstmals einen DS-GVO-konformen Code of Conduct für den Umgang mit personenbezogenen Daten ihrer Kundinnen und Kunden – genehmigt durch die LDI NRW und einstimmig von allen deutschen Datenschutzaufsichtsbehörden mitgetragen.

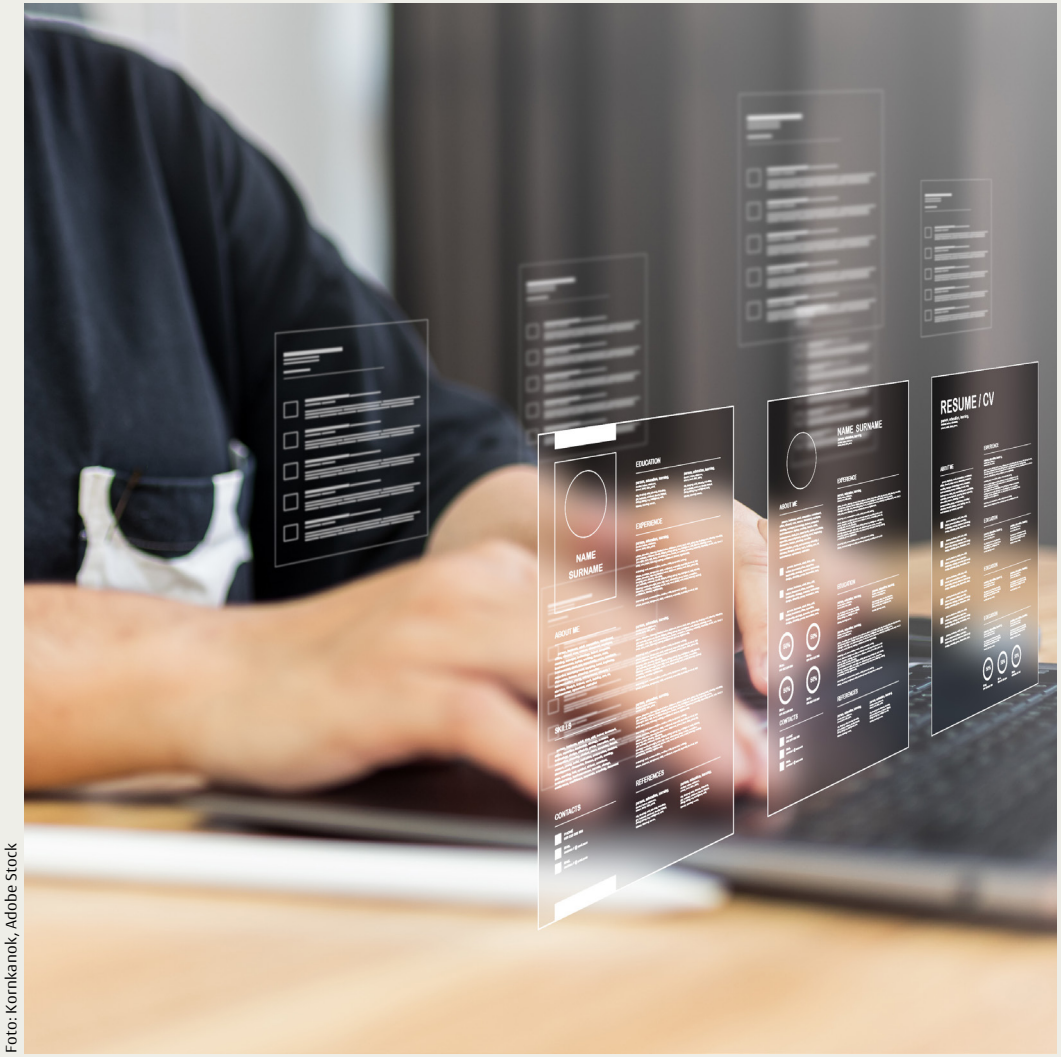


Foto: Kornkanok, Adobe Stock

Die DS-GVO eröffnet Verbänden und Branchenvereinigungen die Möglichkeit, eigene Verhaltensregeln (sog. Codes of Conduct, CoC) zum datenschutzkonformen Umgang mit personenbezogenen Daten zu entwickeln. Diese müssen von der zuständigen Aufsichtsbehörde nach Art. 40 Abs. 5 DS-GVO genehmigt werden und konkretisieren die abstrakten Vorgaben der DS-GVO für das jeweilige Tätigkeitsfeld.

Auf Initiative des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV) wurden entsprechende Verhaltensregeln erarbeitet. Die LDI NRW hat den Entwurf als zuständige Aufsichtsbehörde geprüft und genehmigt (Ziffer 9.4 31. Tätigkeitsbericht Nordrhein-Westfalen LfD 2025). Parallel dazu wurde ein Muster für eine Einwilligungs- und Schweigepflichtentbindungserklärung für die Verarbeitung von Gesundheitsdaten in der Lebens- und Krankenversicherung abgestimmt. Aufgrund der deutschlandweiten Wirkung des CoC wurde der Entwurf mit allen deutschen Datenschutzaufsichtsbehörden beraten. Die DSK hat die Genehmigung einstimmig unterstützt.

Der CoC gilt für sechs Jahre mit einer Evaluierungspflicht nach vier Jahren. Die LDI NRW hat sich einen Widerrufsvorbehalt bei späteren gesetzlichen Änderungen ausdrücklich vorbehalten.

Für Datenschutzbeauftragte und Compliance-Verantwortliche in der Versicherungsbranche liefern die Verhaltensregeln konkrete Handlungsmaßstäbe – insbesondere beim Umgang mit sensiblen Gesundheitsdaten in der Lebens- und Krankenversicherung. Die neuen Verhaltensregeln sowie das abgestimmte Einwilligungsmuster sollten zeitnah in bestehende Datenschutzmanagementsysteme integriert werden.

Schulungspflicht für Geschäftsleitungen nach BSIG

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine aktualisierte Handreichung zur Schulungspflicht für Geschäftsleitungen nach § 38 Abs. 3 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) veröffentlicht. Das Dokument richtet sich an Geschäftsleitungen wichtiger und besonders wichtiger Einrichtungen im Sinne der NIS-2-. E gibt Orientierung zu Inhalt, Format und Nachweis der gesetzlich vorgeschriebenen Schulungen.

Foto: Atchariya63, Adobe Stock

Gesetzlicher Rahmen und Verantwortung

§ 38 BSIG verpflichtet Geschäftsleitungen, Risikomanagementmaßnahmen nicht nur umzusetzen, sondern deren Einhaltung aktiv zu überwachen. Eine Delegation ist ausdrücklich ausgeschlossen. Bei schuldhafter Pflichtverletzung droht persönliche Haftung. Die Schulungspflicht ist klar abzugrenzen von den Mitarbeitendenschulungen nach § 30 Abs. 2 Nr. 7 BSIG.

Schulungsinhalte: drei Kernbereiche

Das BSI benennt drei Pflichtbereiche: Risikoerkennung und -bewertung, Risikomanagementmaßnahmen (inkl. Dokumentationspflichten) sowie Auswirkungsbeurteilung hinsichtlich Verfügbarkeit, Integrität und Vertraulichkeit. Eine Schulung, die sich ausschließlich auf Maßnahmen beschränkt, gilt als unzureichend.

Formate, Intervalle und Nachweis

Das BSI empfiehlt eine ausführliche initiale Schulung mit regelmäßigen Folgeschulungen, orientiert an Risikoexposition und Anlassereignissen. Neben klassischen Formaten werden praxisnahe Ansätze wie Tabletop Exercises oder Audit-Simulationen empfohlen. Die Teilnahme ist intern zu dokumentieren und auf Verlangen nachzuweisen.

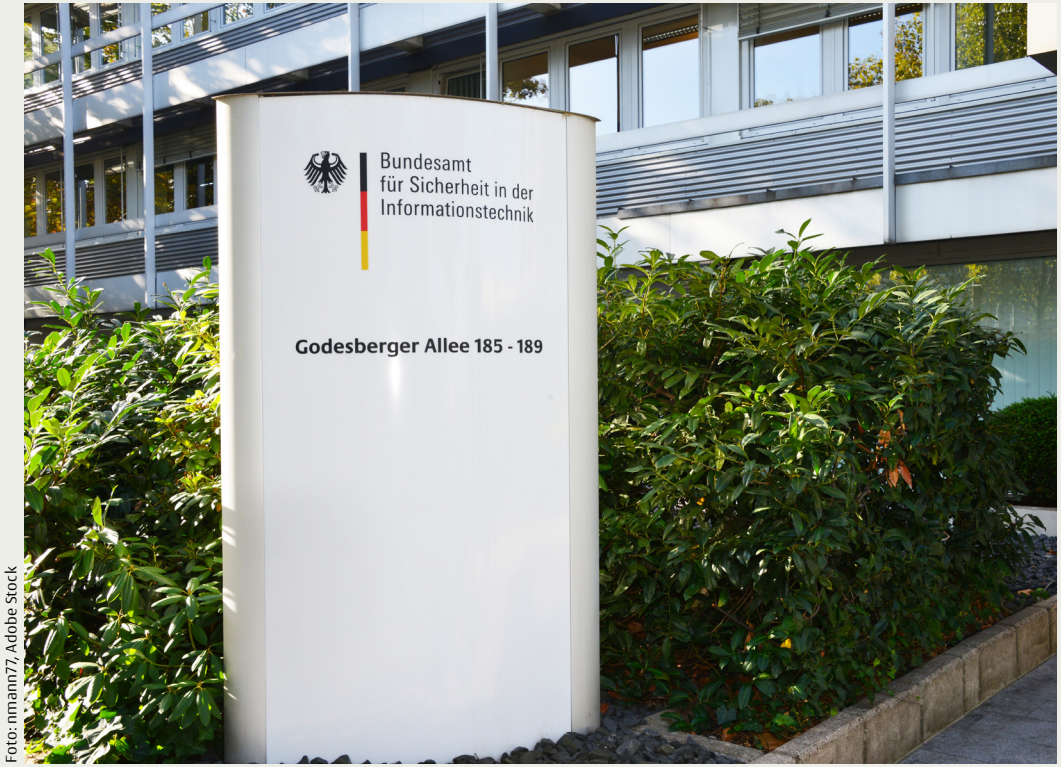


Foto: nmann77, Adobe Stock

BSI veröffentlicht Methodikleitfaden für Grundschutz++

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Anfang April 2026 die erste Version seines Leitfadens zur Methodik des Grundschutz++ veröffentlicht. Das Dokument markiert einen weiteren Schritt bei der Ablösung des klassischen IT-Grundschutzes durch den modernisierten Nachfolgestandard.

Inhalt und Zielsetzung

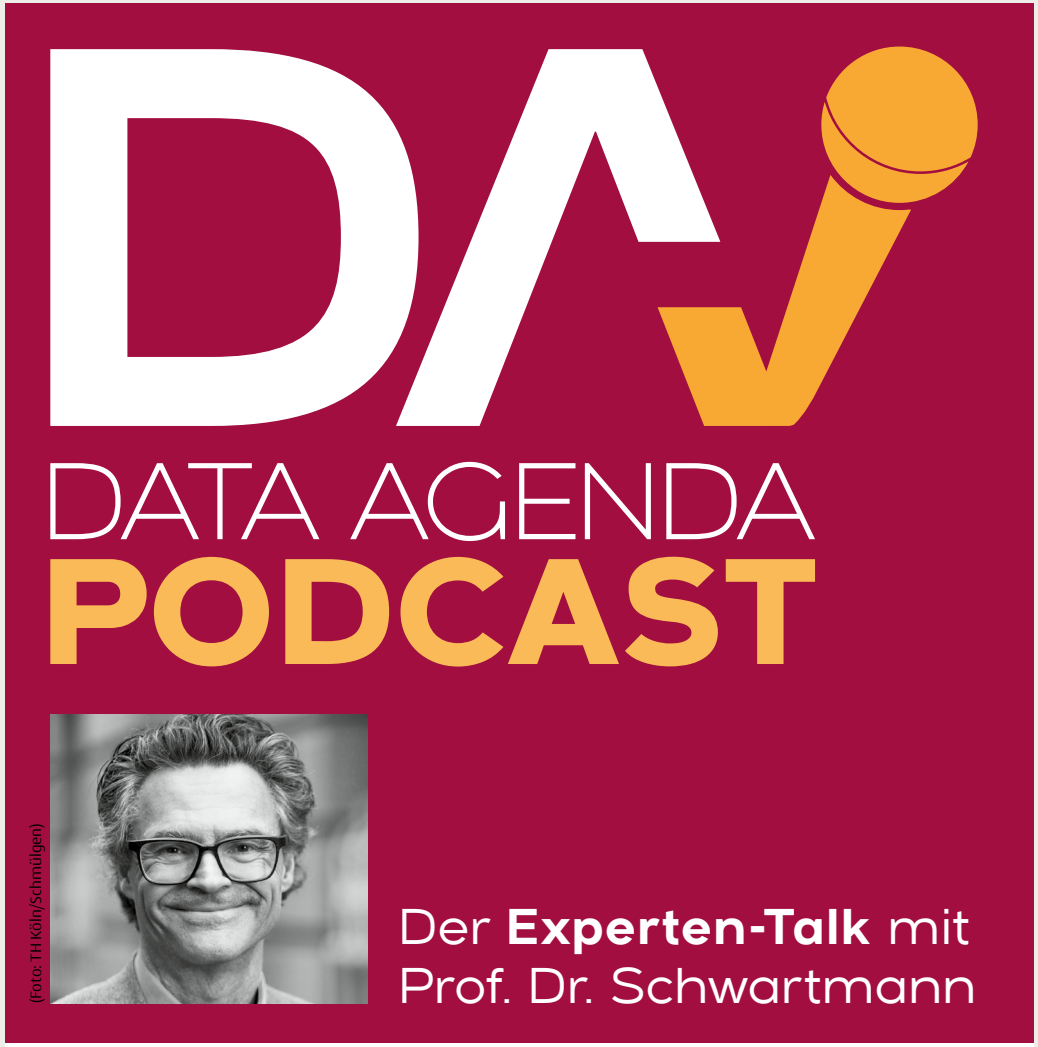
Der Leitfaden bildet einen zukunftsgerichteten Ordnungsrahmen für den systematischen Aufbau und die Weiterentwicklung eines Informationssicherheitsmanagementsystems (ISMS). Er beschreibt eine entlang des PDCA-Zyklus (Plan – Do – Check – Act) strukturierte Methodik, die strategische Verankerung, Anforderungsanalyse, Umsetzung, Überwachung und kontinuierliche Verbesserung zu einem konsistenten Sicherheitsprozess verbindet. Grundschutz++ setzt dabei auf modulare Praktiken und eine prozessorientierte Struktur statt starrer Bausteine sowie auf ein OSCAL/JSON-basiertes, maschinenlesbares Regelwerk, das teilweise automatisierte Compliance-Prüfungen ermöglicht – bei gleichzeitiger Reduktion der Anforderungen um rund 80 Prozent gegenüber dem bisherigen Kompendium.

Eingeschränkte Anwendbarkeit – Pilotprojekte im Fokus

Der Leitfaden ist explizit nur für Pilotprojekte gedacht und nicht für die Migration von Informationsverbünden, die derzeit ein ISMS nach Grundschutz „Edition 2023“ betreiben. Der aktuelle Stand von Grundschutz++ ist bisher nur sehr eingeschränkt praktisch anwendbar, da wesentliche Definitionen und Teile der Methodik noch fehlen – darunter Vorgaben zu Kennzahlen, Blaupausen, Schutzbedarfsbewertung und Modellierung.

Übergangsphase bis 2029

Die Edition 2023 des IT-Grundschutzes bleibt gültig und zertifizierungsrelevant. Eine Übergangsphase bis 2029 ist geplant, in der beide Standards parallel gelten. Mit dem Leitfaden kommt das BSI seiner in der NIS-2-Umsetzungsverordnung festgelegten Pflicht nach, einen neuen „Stand der Technik“ zu definieren, der für alle wichtigen und besonders wichtigen Organisationen verpflichtend ist.
Für Informationssicherheitsbeauftragte (ISB) empfiehlt sich eine frühzeitige Auseinandersetzung mit dem Dokument – insbesondere für NIS-2-betroffene Organisationen, die ein ISMS nach dem vom BSI definierten Stand der Technik neu aufbauen wollen.



Data Agenda Podcast Folge 93: Digitale Souveränität in menschlicher Hoheit

Die Digitale Souveränität Europas ist ein Gebot dieser Zeit. Die menschliche Hoheit in Zeiten zu behalten, in denen KI-Systeme uns das Denken abnehmen können, ist ein anderes. Die Menschen in Europa müssen nun beweisen, dass sie den Herausforderungen gewaschen sind. Die EU und ihre Mitgliedstaaten müssen einen regulatorischen Rahmen schaffen, der Menschenrechte und gute wirtschaftliche Rahmenbedingungen möglich macht.

Im DataAgenda-Podcast spreche ich mit Aljoscha Burchardt vom Deutschen Forschungszentrum für Künstliche Intelligenz über Digitale Souveränität, AI-Companions, die Anforderungen an automatisierte Einzelentscheidungen nach der KI-VO und der DS-GVO und die Ergänzung des Grundgesetzes um das „Staatsziel Mensch“ über mein Buch „Über Leben mit KI. Wie wir uns gegen die Maschine behaupten“, das am 2. Juni erscheint. Ein Leseprobe findet sich in den Shownotes.

Shownotes:

Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Impressum

DATAKONTEXT GmbH
Augustinusstraße 11 A
50226 Frechen

Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Stefan Waldeisen
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299

Newsletter

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen? Dann tragen Sie sich unverbindlich und kostenlos ein unter:
www.datakontext.com/newsletter