ProtectYourIT

Datenschutz-Newsletter – 1 / 2025

Aktuelle Informationen im Bereich Datenschutz

Liebe Kund*innen,

Ich freue mich, Ihnen unser neues Newsletter-Format vorstellen zu können! Ab sofort erhalten Sie unregelmäßig aktuelle Informationen rund um das Thema Datenschutz. Die Anzahl der Newsletter richtet sich nach gesetzlichen Änderungen oder richterlichen Entscheidungen, die Sie betreffen können. Falls eines der Themen für Sie von besonderem Interesse ist, zögern Sie bitte nicht, mich für weitere Details zu kontaktieren.

Aufbewahrungsfristen

Seit dem 1. Januar 2025 gelten neue Aufbewahrungsfristen für Buchungsbelege gemäß § 257 Abs. 4 HGB und § 147 Abs. 3 AO. Die Frist wurde von 10 auf 8 Jahre verkürzt.

Anforderungen für Webshop Betreiber

Der PCI DSS Sicherheitsstandard 4.0 beschreibt Sicherheitsanforderungen an Webshops, die Onlinezahlungen ermöglichen. Dieser Standard ist 2024 in Kraft getreten und bringt die Anforderung mit sich, dass die Betreiber regelmäßige PCI-konforme Schwachstellen Scans durchführen müssen. Diese Anforderung wird von einigen Zahlungsanbietern restriktiv ausgelegt und kann kostenintensiv sein. Stimmen Sie sich hierzu mit Ihrem Webshopanbieter ab.

NIS-2

Dieses Gesetz zur Umsetzung der EU-Richtlinie 2022/2555 zur Cybersicherheit sollte bereits im Oktober 2024 in Deutschland umgesetzt sein. Jedoch konnte die alte Bundesregierung das Gesetz nicht verabschieden und ein neuer Termin steht noch nicht fest. Dieses Gesetz wird direkt oder indirekt (für Organisationen innerhalb einer Lieferkette mit direkt betroffenen Organisationen) Anforderungen an die Verbesserung der Cybersecurity stellen. Dies beinhaltet ein dokumentiertes Risikomanagement, ein Incidentmanagement und die unter „Notfallvorbereitung“ beschriebenen Maßnahmen.

Cyber Resilience Act (CRA)

Diese EU-Verordnung wird 2025 in Kraft treten und neue Anforderungen an Produkte mit digitalen Elementen stellen. Produkte mit digitalen Elementen, wie bspw. Smartphones, Smart Home-Geräten, Fahrzeuge, medizinische Geräte, industrielle Maschinen müssen deren Sicherheit und Widerstandsfähigkeit gegen Cyberangriffe erhöhen. Der CRA betrifft alle Unternehmen, die solche Produkte herstellen, importieren oder vertreiben.

Barrierefreiheitsstärkungsgesetz (BFSG)

Am 28. Juni 2025 tritt das Barrierefreiheitsstärkungsgesetz (BFSG) in Kraft. Es bringt neue Pflichten für alle, die z.B. “smarte” Produkte vertreiben oder E-Commerce-Angebote, wie z.B. Onlineshops betreiben. Das Ziel des Gesetzes, dass Personen mit Behinderungen gleichwertig an digitalen Inhalten und digitalem Konsum teilhaben können. RA Dr. Schwenke hat hierzu einen sehr hilfreichen Ratgeber mit FAQs veröffentlicht: https://datenschutz-generator.de/bfsg-ratgeber/

Künstliche Intelligenz

Die EU-Verordnung 2024/1689 (KI-VO) regelt den Einsatz von KI. Das Gesetz ist noch nicht vollständig in Kraft getreten. Organisationen mit KI-Systemen, die wahrscheinlich als Hochrisiko eingestuft werden, sollten sich jetzt schon bei der zuständigen Aufsichtsbehörde registrieren.

Ein weiterer Punkt ist die KI-Nutzung innerhalb der Organisation und ich empfehle dringend die Mitarbeitenden anhand einer KI-Regelung zu sensibilisieren, damit personenbezogene Daten und Geschäftsgeheimnisse nicht durch Nutzung freier KI-Tools verloren gehen.

Wenn Sie das Thema KI interessiert und Sie fundierte und weiterführende Informationen haben wollen, kann ich Ihnen die Leistungen von Dr. Koglin von LegalCheck empfehlen. Weitere Informationen finden Sie unter: https://www.legalcheck.de/ki-fachkunde

Windows 10 Supportende

Ab dem 14. Oktober 2025 wird der Support für Windows 10 eingestellt. Unternehmen sollten auf Windows 11 umsteigen oder alternative Lösungen wie das ESU-Programm von Microsoft in Betracht ziehen.

World Backup Day

Am 31. März 2025 wurde der World Backup Day begangen, um die Sensibilität für Datensicherungen zu steigern. Die aktuellen Empfehlungen beschreiben über das 3-2-1-1-0 Konzept hinaus die Trennung der Datensicherungssysteme vom übrigen Netzwerk und Einschränkung der Zugriffsmöglichkeiten, eine Absicherung gegenüber Ransomware und die regelmäßige Kontrolle der Vollständigkeit sowie Wiederherstellungstests.

Notfallvorbereitung

Der Bericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur IT-Sicherheit in Deutschland 2024 zeigt weiterhin eine angespannte Lage. Cyberkriminelle nutzen zunehmend Zero-Day-Schwachstellen und Ransomware-Angriffe nehmen zu. Unternehmen sollten sich auf Notfälle vorbereiten, indem sie Risiken identifizieren und Maßnahmen zur Risikominderung ergreifen. Dazu gehören ein Notfallhandbuch oder ein Business Continuity Management sowie Awareness Schulungen. Diese Maßnahmen werden zudem von Cyberversicherung eingefordert.

Rechtsprechung

- Das Bundessozialgericht entschied, dass eine verspätete Auskunft nach Art. 15 DSGVO keinen Schadensersatz rechtfertigt, wenn kein tatsächlicher Schaden nachgewiesen werden kann.
- Ein Urteil des LG Hagen besagt, dass eine Cyberversicherung nicht für Schäden durch gefälschte E-Mails aufkommt, wenn die Systeme des Versicherungsnehmers nicht betroffen sind.
- Der Europäische Gerichtshof entschied, dass Betriebsvereinbarungen die Standards der DSGVO nicht unterschreiten dürfen. Nationale Gerichte können die Regelungen einer Betriebsvereinbarung vollumfänglich überprüfen.

Schöne Grüße,

Stephan Krischke