ProtectYourIT

Datenschutz & Compliance – *Brief-IT*
1 / 2026

Liebe Kund*innen,

Sie erhalten in unregelmäßigen Abständen aktuelle Informationen rund um das Thema Datenschutz, Informationssicherheit & Compliance. Falls eines der Themen für Sie von besonderem Interesse ist, zögern Sie bitte nicht, mich für weitere Details zu kontaktieren.

Cyber Resilience Act (CRA):

Die **CE-Kennzeichnung für Cybersecurity** wird ab Dezember 2027 verpflichtend und es dürfen **nur noch CRA-konforme** Produkte (Hard- & Software) neu in Verkehr gebracht werden. Sichtbares Zeichen der Konformität ist eine CE-Kennzeichnung der Produkte. Meine klare **Empfehlung** an Sie ist schon jetzt bei der **Beschaffung neuer IT-Infrastruktur** die **CRA-Konformität** der Produkte für 2027 **einzufordern**, um Sicherheitsrisiken, Nachrüstungsstress und -kosten zu minimieren. Die CRA-Konformität sollte **schriftlich** eingefordert werden und Aussagen, die Hersteller von Security-Pflichten entbinden oder Haftung auf Sie abwälzen sollten nicht akzeptiert werden.

NIS2:

Die NIS2 ist am 5. Dezember 2025 in Kraft getreten und die **Frist** zur **Registrierung** beim Bundesamt für Sicherheit in der Informationstechnologie (BSI) ist am **6. März 2026 abgelaufen**. Viele der geschätzten 45.000 betroffenen Unternehmen sind dieser Verpflichtung nicht nachgekommen. Nach der Registrierung steht nun die Planung und Umsetzung der Maßnahmen auf der Agenda und insbesondere die Einhaltung der **Meldefristen** für **Sicherheitsvorfälle** sorgt für Diskussion. Die **24** Stundenfrist für die **Erstmeldung** bezieht sich auf den Zeitpunkt des **Bekanntwerdens** eines Sicherheitsvorfalls. Dies bezieht sich auf die **Kernarbeitszeiten** der Organisation und beinhaltet nicht die Bereitstellung eines 24x7 IT-Betriebes.

Zudem sind **IT-Dienstleister**, die für den **IT-Betrieb** einer Organisation beauftragt und somit für diesen **verantwortlich** sind, sollten **schriftlich** zur Einhaltung der Meldefrist **verpflichtet** werden und ein **Prozess** ist dafür zu **etablieren**, damit die/der Informationssicherheitsbeauftragte zeitnah informiert wird.

KI-Verordnung (AI-Act):

Wie bereits berichtet, sind in 2025 die **Bundesnetzagentur** als zuständige **KI-Aufsichtsbehörde** benannt und die Anforderung **Mitarbeitende** im Umgang mit **KI** zu **schulen** ist in Kraft getreten. Die Anzahl der KI-Anbieter nimmt stetig zu und aktuell liegt der Fokus in der effizienteren Gestaltung internen Geschäftsprozesse mit KI-Unterstützung. Dieses Jahr wird die vorletzte Stufe der AI-Act Umsetzung voraussichtlich am **2. August** in Kraft treten. Die damit verbundenen Pflichten umfassen die **Kennzeichnung KI-generierter Inhalte** und die **Informationspflichten** gegenüber **Betroffenen**, wenn Daten mit der **KI verarbeitet** werden.

Die Pflichten beinhalten aber auch, dass KI-Systeme in **kritischen Bereichen** (in Annex III gelistet) – z. B. **Medizinprodukte-KI**, **Recruiting- und Personal-Software**, **KI in Fahrzeugen**, **Justiz & Asyl** die

umfangreichen Anforderungen als **Hochrisiko KI-System** erfüllen müssen und dieses System **registriert** haben. Sofern Sie ein System in diesem Bereich **einsetzen** wollen, ist vom **Anbieter** eine Stellungnahme zur **Risikobewertung einzufordern**.

Für **KI-generierte Inhalte** wird in **Deutschland** eine **Leitlinie** zur Kennzeichnung (z. B. Werbe-/Influencer-Bereich) von der **Wettbewerbszentrale** (02/2026) angeboten. Sie sollten dies bereits jetzt implementieren, wenn in Ihrer Organisation KI-erzeugter Content, Chatbots oder virtuelle Assistenten im Dialog angeboten werden: https://www.wettbewerbszentrale.de/wettbewerbszentrale-veroeffentlicht-leitfaden-zur-ki-kennzeichnung/

Der Bayerische Landesbeauftragte für den Datenschutz (**BayLfD**) veröffentlichte am 1.3.2026 auf seiner Webseite unter der Rubrik „Künstliche Intelligenz (KI)“ eine umfassende **Orientierungshilfe** zu datenschutzrechtlichen Anforderungen beim Einsatz von KI-Systemen in **bayerischen öffentlichen Stellen** veröffentlicht: https://www.datenschutz-bayern.de/ki/OH_KI.pdf

Aufsichtsbehörden und Verbände

Die nichtendend wollende Überprüfung der deutschen Aufsichtsbehörden zum **Einsatz** von **M365** hat Ende 2025 eine neue Richtung eingeschlagen. Der Hessische Datenschutzbeauftragte (HBDI) kam nach Verhandlungen mit Microsoft zum Schluss, dass M365 unter **bestimmten Bedingungen** datenschutzkonform eingesetzt werden kann. Notariats- und Anwaltsverbände (BRAK und BNotK) sehen den Einsatz noch positiver, da derzeit keine Beanstandungen bekannt sind. Zusammengefasst wird ein **Konzept** zur risikobasierten Umsetzung **technisch-organisatorischer Maßnahmen empfohlen**. Damit wächst der **Trend**, um M365 unter **Auflagen in Organisationen mit besonders schützenswerten Daten einsetzen** zu können.

Gesetzliche Änderungen

Widerrufsbutton im **B2C e-Commerce**: Ab dem 19. Juni 2026 ändert sich der § 356a BGB und **verpflichtet** alle Händler, Dienstleister und andere Unternehmen im B2C-Onlinehandel, eine elektronische **Widerrufsfunktion** bereitzustellen – den sogenannten Widerrufsbutton. Eine detaillierte Checkliste findet sich unter: https://datenschutz-generator.de/widerrufsbutton/

Der **„digitale Omnibus“** bezeichnet ein umfassendes EU-Gesetzespaket (vorgestellt Ende 2025), das zahlreiche bestehende Digitalgesetze durch gezielte technische Anpassungen **vereinheitlichen** und **vereinfachen** soll. Bspw. soll damit die DSGVO-Meldepflicht bei **Datenschutzverletzungen** von derzeit 72 auf 96 Stunden verlängert werden. Der **Bundesrat** hat die geplanten Reformen begrüßt, zugleich jedoch an mehreren Stellen deutlichen **Nachbesserungsbedarf** betont. Die **Verhandlungen** werden auf EU-Ebene im **Sommer** weitergeführt, ein Termin zur Umsetzung steht aktuell noch nicht fest.

Einen guten Start in den Mai wünscht,

Stephan Krischke