ProtectYourIT

Datenschutz & Compliance - Newsletter 3 / 2025

Liebe Kund*innen,

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

EU-Streitbeilegungsplattform wurde **abgeschaltet**: Zum 20. Juli 2025 wurde die Plattform zur Online-Streitbeilegung der EU (OS-Plattform) endgültig abgeschaltet. Um dadurch nicht in eine Abmahnfalle zu tappen, müssen Betreiber den Link aus Ihrer Webseite/dem Webshop (z.B. **Impressum**, **AGBs**) entfernen. Findet sich der Link ab dem 20. Juli 2025 weiterhin im Webshop/auf der Webseite, kann dies zukünftig als Verbrauchertäuschung gewertet werden: Mit dem Hinweis auf die OS-Plattform wird dann irreführend eine Möglichkeit der Streitbeilegung vorgetäuscht, die es so nicht mehr gibt.

Lizenzpflichtige Schriftarten auf der Webseite: **Lizenzkontrollen** kostenpflichtiger Schriftarten im Internet sind zunehmend automatisiert und professionell organisiert. Spezialisierte Tools und Rechtsdienstleister überwachen aktiv Font-Nutzung weltweit und in letzter Zeit hat bspw. **Monotype** Unternehmen zur Zahlung von Lizenzgebühren aufgefordert. Überprüfung Sie zusammen mit Ihrem Webdesigner die auf Ihrer Webseite genutzten Schriftwarten, um sicher zu gehen.

Workation bedeutet, Arbeit und Urlaub zu kombinieren: Dieses Arbeitsmodel wird immer beliebter, denn damit wir die Arbeit ortsunabhängig durchgeführt, und nutzt die Freizeit für Erholung am Urlaubsort. Ziel ist es, Produktivität und Entspannung zu verbinden, wobei eine stabile und sichere Internetverbindung und einige regulatorische Anforderungen entscheidend sind. Sofern Sie dieses Arbeitsmodel einführen wollen, sollten Sie **verbindliche Regeln** aufstellen, einschließlich Vorgaben zur Aufenthaltsdauer, IT-Nutzung und dem technischen Rahmen. Innerhalb der EU/EWR/Schweiz gilt das als „Entsendung“ und es ist darauf zu achten, dass der Arbeitgeber eine **A1-Bescheinigung** beantragt, damit der Mitarbeitende weiterhin dem deutschen Sozialversicherungsrecht unterliegt.

Löschverfahren nach DIN 66399: Die bisher gültige DIN 66399 zur Löschung und Vernichtung von Daten wurde aufgrund der internationalen Harmonisierung zurückgezogen und durch die Norm **ISO/IEC 21964 ersetzt**. Diese Norm regelt künftig die Anforderungen an die sichere Löschung und Vernichtung von. Bitte prüfen Sie alle internen Richtlinien und Verträge auf Verweise zur DIN 66399 und passen Sie diese bei Bedarf an.

Teams – Arbeitsort-Erkennung: In Microsoft Teams lässt sich der Standort wie Büro oder Remote festlegen und bei Bedarf teilen. Kürzlich wurde eine automatische Erkennung eingeführt, bei der Teams über Wifi, IP oder Firmennetz erkennt, ob man im Büro ist. Der Dienst stellt dann selbst ein, ob Nutzer als Remote oder Office angezeigt werden. Diese Funktion muss vom IT-Administrator **aktiviert** werden.

Die Verarbeitung von Standortdaten setzt in der Regel eine Einwilligung voraus, da der Arbeitsvertrag meist keine Kontrolle des Arbeitsortes erlaubt. Ausnahmen gelten nur, wenn die Standortkontrolle für die Arbeit notwendig ist. Eine pauschale Annahme von Datenschutzverstößen ist daher nicht korrekt – entscheidend ist der Zweck der Datennutzung. In Deutschland sollte die Standortfunktion grundsätzlich **deaktiviert bleiben** und darf nur mit Zustimmung von Betriebsrat aktiviert werden; dabei muss Freiwilligkeit sichergestellt sein.

Es ist so weit, **NIS2** tritt in Kraft! Das Gesetz wurde am **6. Dezember 2025** vom Bundestag und Bundesrat verabschiedet und tritt sofort nach der Veröffentlichung in Kraft. Sie sollten – falls noch nicht geschehen - jetzt prüfen, ob sie direkt oder indirekt davon betroffen sind, und die nötigen Maßnahmen planen – besonders, wenn sie Teil einer NIS2-Lieferkette sind. Wichtiger **Hinweis**: Die Geschäftsführung haftet persönlich bei Verstößen.

Cyber Resilience Act (CRA): Im letzten Newsletter wurde bereits auf den CRA hingewiesen. Zwischenzeitlich erfolgte eine umfassendere Auseinandersetzung mit dem Thema. Das Gesetz hat weitreichende Auswirkungen, da es nahezu alle im Alltag genutzten IT-Geräte sowie Unternehmen betrifft, die Produkte herstellen oder als Whitelabel vertreiben. Die Umsetzung des CRA ist bis Ende 2027 verpflichtend; ein frühzeitiger Beginn wird empfohlen, da einzelne Anforderungen sehr komplex sein können. Ähnlich wie bei der Einführung der DSGVO besteht das Risiko, dass sich die Situation zum Ende hin **zuspitzt**. Es wird allen Unternehmen geraten, eine aktuelle **Inventarliste** zu führen, um frühzeitig mit Anbietern wichtiger Komponenten Kontakt aufzunehmen und entsprechende Informationen einzuholen. Anbieter von Produkten im Geltungsbereich des CRA sollten sämtliche Anforderungen für ihre Produkte und gegebenenfalls Ersatzteile sorgfältig **prüfen**.

Künstliche Intelligenz: In Deutschland gibt es derzeit keine zuständige Aufsichtsbehörde für KI-Überwachung, sodass noch **keine Bußgelder** verhängt werden. Das Omnibus IV Paket der EU wurde im Dezember 2025 verabschiedet und **entlastet** besonders kleine und mittlere Unternehmen, indem es Fristen zur Umsetzung des AI-Acts verschiebt. **Hochrisiko-KI-Systeme** müssen aber weiterhin bis August 2026 die Anforderungen erfüllen. Wer solche Systeme in Bereichen wie Biometrie, kritische Infrastrukturen, Bildung, Personal oder Gesundheitsdienste nutzt, muss eine Risikobewertung durchführen.

Eine schöne Vorweihnachtszeit wünscht,

Stephan Krischke