ProtectYourIT

Datenschutz & Compliance - Newsletter 2 / 2025

Liebe Kund*innen,

schon mit dem Versand des zweiten Newsletters habe ich eine Änderung des Formats vorgenommen. Sie erhalten in unregelmäßigen Abständen aktuelle Informationen rund um das Thema Datenschutz & Compliance. Viele der gesetzlichen und regulatorischen Anforderungen haben eine Überschneidung mit dem Datenschutz. Falls eines der Themen für Sie von besonderem Interesse ist, zögern Sie bitte nicht, mich für weitere Details zu kontaktieren.

SEPA-Überweisungen

Ab dem **9. Oktober 2025** müssen Banken im europäischen Zahlungsraum bei SEPA-Überweisungen und SEPA-Echtzeitüberweisungen eine sogenannte **Verification of Payee (VoP)** durchführen. Das bedeutet, dass vor jeder Autorisierung einer Überweisung geprüft wird, ob der Name des Empfängers mit der IBAN übereinstimmt. Diese Maßnahme soll helfen, betrügerische oder fehlgeleitete Zahlungen zu verhindern und den Schutz des Zahlers zu erhöhen.

Ihre Banken haben Sie sicherlich schon über diese Veränderung informiert, jedoch möchte ich nochmal empfehlen, dass Sie die Namen aller **Empfänger** in Ihren Stammdaten **überprüfen**.

DATEV Personal

Unternehmen, die Ihre **Personalstammdaten** und digitalen **Personalakten** in DATEV Unternehmen online im Zusatzmodul **DATEV Personal** verwalten, müssen einen **Auftragsverarbeitungsvertrag** direkt mit DATEV abschließen. Dies ist auch dann erforderlich, wenn DATEV über Ihren Steuerberater bereitgestellt wird. Hintergrund ist, dass diese Leistung nicht mehr unter der weisungsfreien Tätigkeit des Steuerberaters fällt und gesondert geregelt werden muss.

Sofern dies Ihr Unternehmen betrifft, bitte ich Sie um eine **Rückmeldung**.

NIS-2

Die Umsetzung der NIS-2 zieht sich auch mit der neuen Regierung hin und aktuell wird mit **Anfang 2026** für das Inkrafttreten des Gesetzes gerechnet. In den letzten Monaten wurden noch einige Anforderungen nachgebessert, so ist die Meldefrist etwas entschärft worden und lediglich die **Erstmeldung** der Sicherheitsvorfälle für direkt betroffene Unternehmen hat beim BSI innerhalb von 24 Stunden zu erfolgen. Eine weitere Erleichterung betrifft die Unternehmen mit **irrelevanten Nebentätigkeiten** in NIS2-Sektoren. Diese sollen nicht reguliert werden, d.h. wenn Leistungen nicht zu den Hauptprodukten des Unternehmens zuzurechnen sind, sind die NIS-2 Anforderungen nicht direkt umzusetzen.

Eine wichtige Anforderung sollten alle Geschäftsleitungen mit der Entscheidung, ob NIS-2 die Organisation betrifft, berücksichtigen: Die **Geschäftsleitung haftet persönlich** bei Verstößen.

Cyber Resilience Act (CRA)

Bereits 2024 ist der CRA in Kraft getreten und die Umsetzungsphase dauert noch bis 2027 an. Der CRA umfasst alle **Produkte** mit **digitalen Elementen** (bspw. SmartWatch, „connected“ KFZ, IoT-Geräte, digitale Maschinensteuerung) und legt umfangreiche Anforderungen für Unternehmen, die Hersteller, Händler und Softwareanbieter dieser Produkte sind, fest. Am Ende der Anforderungsliste steht eine

Konformitätsbescheinigung, die einer CE-Kennzeichnung entspricht und je nach Risikoeinstufung der Produkte intern oder durch Prüforganisationen erstellt werden muss.

Diese Anforderung wird auch fast alle Anbieter von **IT-Systemen** (Firewalls, Virenschutz, Clouddienste etc.) betreffen und somit wird der IT-Systembereich zukünftig auch Cybersecurity Anforderungen erfüllen müssen.

Barrierefreiheitsstärkungsgesetz (BFSG)

Am 28. Juni ist das Barrierefreiheitsstärkungsgesetz (BFSG) in Kraft getreten. Das Gesetz richtet sich an **private Unternehmen,** die Produkte oder Dienstleistungen auf Webseiten oder Portalen für **Verbraucher** anbieten und an **öffentliche Einrichtungen**, die teilweise noch erweiterte Pflichten erfüllen müssen. RA Dr. Schwenke hat hierzu einen umfangreichen **Praxisratgeber** veröffentlicht: https://datenschutz-generator.de/wp-content/uploads/2025/06/Whitepaper_BFSG_schwenke_v1.0.pdf

Künstliche Intelligenz

Die Verwendung von KI in den **täglichen Arbeitsabläufen** nimmt stetig zu. Organisation die KI zur Unterstützung der Geschäftsprozesse verwenden, müssen darauf achten, dass die **Datenschutzanforderungen** eingehalten werden. Der Datenschutz kommt im Zusammenhang mit KI zur Anwendung, wenn **personenbezogene Daten** mit der KI verarbeitet werden. Darunter fallen bspw. auch E-Mailadressen und IP-Adressen sowie pseudonymisierte Daten. Falls Sie personenbezogene Daten mit Hilfe der KI verarbeiten, muss eine **rechtliche Grundlage** dafür vorhanden sein und die betroffenen Personen müssen darüber **informiert** werden.

Organisationen sind zudem in der Verantwortung, Personal ausreichend hinsichtlich der **KI-Kompetenz** zu schulen. In der Praxis stehen die **Schulungen** in Abhängigkeit von der Art und dem Umfang der genutzten KI-Systeme, d.h. es sind nur die Personen zu schulen, die KI verwenden und der Schulungsinhalt ist von dem Risiko des genutzten KI-Systems abhängig. Eine gesetzliche Verpflichtung zur Benennung eines **KI-Verantwortlichen** besteht nicht.

Rechtsprechung

Ende Mai erlaubte das OLG Köln Meta, die Daten der Facebook- und Instagram-Nutzer für KI-Trainingszwecke einzusetzen, solange die Nutzer nicht widersprechen. Bei derart unternehmensfreundlicher Rechtsprechung ist es kein Wunder, dass andere Plattformen, wie jetzt **LinkedIn**, nachziehen. Wenn Sie jedoch nicht möchten, dass LinkedIn Ihre Daten für **KI-Training** nutzt, schalten Sie diese Option bis zum 03. November 2025 in Ihren **Einstellungen** ab. Es sei denn, Sie versprechen sich Vorteile davon, Ihre Daten zu teilen.

Das VG Köln hat mit dem Urteil vom 17.7.2025 entschieden, dass das Presse- und Informationsamt der Bundesregierung (BPA) seine **Facebook-Seite** weiterhin betreiben darf. Damit wurde eine Weiche für die Nutzung sozialer Medien in **öffentlichen Einrichtungen** gestellt, um zusätzliche Kommunikationskanäle zu den Bürgern zu öffnen.

Schöne Grüße,

Stephan Krischke