Newsletter November 2024
Knyrim Trieb Rechtsanwälte OG

Sehr geehrte Damen und Herren!
Liebe Datenschutzinteressierte!

Unser aktueller Newsletter bietet Ihnen Informationen und Wissenswertes aus der Welt des Datenschutzes, diesmal mit Fokus auf künstliche Intelligenz.

Erste Pflichten und Verbote aus dem AI Act ab 2.2.2025 in Kraft!

Beitrag verfasst von Dr. Rainer Knyrim – KTR-Newsletter November 2024

Der AI Act (dt. Verordnung über künstliche Intelligenz, kurz „KI-Verordnung“) wird bis August 2026 in drei Phasen anwendbar. Die erste Phase beginnt am 2.2.2025 mit der Anwendbarkeit der Kapitel I und II. Kapitel I enthält in Artikel 4 eine Verpflichtung zur KI-Kompetenz. Artikel 2 regelt, welche KI-Anwendungen ab 2.2.2025 verboten sind.

I. KI-Kompetenz:

Artikel 4 AI Act verpflichtet Anbieter und Betreiber, intern KI-Kompetenz zu schaffen. Betreiber sind all jene, die KI in ihrer Organisation bloß anwenden, egal welchen Risikograd die KI hat, d.h. die Verpflichtung gilt auch beim Einsatz von KI mit bloß minimalem Risiko.

Worum geht es bei der Pflicht zur KI-Kompetenz?

Anbieter und Betreiber müssen sicherstellen, dass ihr Personal und jenes ihrer Auftragsverarbeiter, die KI-Systeme betreiben, über ein ausreichendes Maß an Kompetenz im Bereich KI verfügen, wobei diesbezüglich deren

- technische Kenntnisse,
- Erfahrung,
- Ausbildung und Schulung

zu berücksichtigen sind. Weiters sind dabei zu beachten

- der Kontext, in dem die KI-System eingesetzt werden sollen und

- die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen.

In der Praxis bedeutet dies, dass Mitarbeiterinnen und Mitarbeiter, die noch keine ausreichenden technischen Kenntnisse und Erfahrungen haben, für die KI-Anwendung ausgebildet oder geschult werden müssen.

Unsere Kanzlei bietet auf Wunsch hausinterne Schulungen zum Thema KI an, erst kürzlich haben wir die Software-Abteilung eines Unternehmens in Oberösterreich geschult und dort zahlreiche Praxisfragen und Use Cases zu KI durchgearbeitet.

Weiters empfiehlt es sich, im Unternehmen eine **Policy für die Verwendung von KI** zu implementieren, auch wenn dies keine explizite Verpflichtung des Artikel 4 AI Act ist. Auch bei der Erstellung einer Policy unterstützen wir gerne.

II. Ab 2.2.2025 verbotene KI-Anwendungen:

Die Verbote sind in Kapitel II AI Act geregelt, der nur aus einem einzigen Artikel besteht, nämlich dem Artikel 5. Dieser enthält eine Liste an Praktiken, die im KI-Bereich ab 2.2.2025 verboten sind. Die Liste gliedert sich in Verarbeitungen, die typischerweise vor allem in der Privatwirtschaft stattfinden (aber auch im öffentlichen Bereich eingesetzt werden können) und solche, die typischerweise nur dem öffentlichen Sektor vorbehalten sind.

Verbotene KI-Systeme vor allem im privatwirtschaftlichen Bereich:

- KI-Systeme, die Personen beeinflussen, indem unterschwellige Techniken zur Beeinflussung oder absichtlich manipulative oder täuschende Techniken eingesetzt werden, mit dem Ziel oder der Wirkung, das Verhalten einer Person oder einer Gruppe wesentlich zu verändern und dabei ihren freien Willen zu umgehen, wodurch ihr ein erheblicher Schaden zugefügt wird oder werden kann;
- KI-Systeme, die die Schwächen von Menschen (z.B. aufgrund ihres Alters, ihrer Behinderung oder sozialen oder wirtschaftlichen Situation) ausnutzen, wodurch diesen ein erheblicher Schaden zugefügt wird oder werden kann;
- KI-Systeme, die Personen oder Gruppen auf Grundlage ihres sozialen Verhaltens oder persönlicher Eigenschaften oder Merkmale bewerten oder klassifizieren, wobei die dadurch hergeleitete soziale Bewertung zu einer Schlechterstellung oder Benachteiligung dieser Personen oder Gruppen führt (sog. Social Scoring);
- KI-Systeme, die gezielt Gesichtsbilder aus dem Internet oder aus Überwachungsaufnahmen auslesen, um Gesichtserkennungsdatenbanken zu erstellen;
- KI-Systeme, die Emotionserkennung von Personen am Arbeitsplatz oder in Bildungseinrichtungen durchführen (mit Ausnahmen im medizinischen Bereich oder aus Sicherheitsgründen - Letzteres könnte z.B. Müdigkeitserkennung etwa von Piloten oder Berufskraftfahrern sein);
- KI-Systeme, die biometrische Kategorisierungen von Personen durchführen, um deren Rasse, politische Einstellung, Gewerkschaftszugehörigkeit, religiöse oder weltanschauliche Überzeugung, Sexualleben oder sexuelle Ausrichtung daraus abzuleiten (mit Ausnahme im Bereich der Strafverfolgung).

Verbotene KI-Systeme im öffentlichen Bereich:

- KI-Systeme, die Risikobewertungen auf Grundlage von Profiling oder Bewertung persönlicher Merkmale durchführen und damit eine Risikobewertung vornehmen, ob eine natürliche Person künftig eine Straftat begehen wird;

- KI-Systeme, die die biometrische Echtzeit-Fernerkennung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken durchführen (mit Ausnahmen, z.B. bei vermissten Kindern, Tätern bei bestimmten Straftaten).

Wir empfehlen daher, die eigenen IT-Systeme dahingehend zu prüfen, ob die oben genannten verbotenen Praktiken mit diesen möglich sind, etwa im Bereich **Marketing oder bei der Implementierung von Websites im Hintergrund. Ebenso ob elektronische Systeme, die am Arbeitsplatz im Einsatz sind, Emotionen von Mitarbeitern auswerten, etwa in Call Centern durch Spracherkennung; in der Korrespondenz oder in Chats durch semantische Erkennung von Schreibmustern oder in Videokonferenzen durch Bildauswertung**. Gerne stehen wir für eine Beurteilung, ob solche verbotenen Praktiken vorliegen, zur Verfügung.

KI und Datenschutz – Infos und Tipps von DSB und DSK

Beitrag verfasst von Dr. Rainer Knyrim und Fabian Jelicic – KTR-Newsletter November 2024

Künstliche Intelligenz (KI) bringt zahlreiche datenschutzrechtliche Herausforderungen mit sich. Die österreichische Datenschutzbehörde (DSB) hat auf ihrer Website zu diesem Thema FAQ veröffentlicht (https://www.dsb.gv.at/download-links/FAQ-zum-Thema-KI-und-Datenschutz.html), während von der Deutschen Datenschutzkonferenz (DSK) im Mai 2024 eine Orientierungshilfe herausgegeben wurde (https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf).

Die von der EU im Juni 2024 beschlossene Verordnung 2024/1689 („KI-Verordnung" bzw. „AI Act") bildet den zentralen rechtlichen Rahmen für den Einsatz von KI (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401689).

Die **FAQ der DSB** mit Stand vom 2.7.2024 stützen sich auf die Definition in Art 3 Z 1 KI-VO, der künstliche Intelligenz als ein Computersystem beschreibt, das autonom arbeitet, anpassungsfähig ist und Aufgaben erfüllen kann, für die üblicher Weise menschliche Intelligenz notwendig ist. Die DSB weist auf die laut Art 2 Abs 7 KI-VO **parallele Anwendbarkeit der DSGVO** hin, wenn personenbezogene Daten von KI-Systemen verarbeitet werden. Sie hält auch fest, dass sie für alle datenschutzrechtlichen Fragen im Zusammenhang mit KI-Systemen zuständig ist.

Die FAQ betonen, dass die Grundsätze des Art 5 DSGVO beim Einsatz von KI-Systemen einzuhalten sind. Verantwortliche, die eine KI-Anwendung nicht selbst entwickeln, müssen sicherstellen, dass der Anbieter ausreichende Informationen bereitstellt, um die **Transparenzpflichten gemäß Art 12 ff DSGVO** zu erfüllen. Im Rahmen der Transparenzpflichten ist zu prüfen, ob **Ein- und Ausgabedaten** für das Training einer KI verwendet werden. In einem solchen Fall sind die Nutzer ausreichend darüber zu informieren und es ist ihnen die Möglichkeit zu geben, die Nutzung ihrer Daten für das Training auszuschließen. Wenn ein Ausschluss nicht möglich ist und personenbezogene Daten von der Verarbeitung betroffen sind, bedarf es einer Rechtsgrundlage.

Zudem legen die FAQ einen besonderen Fokus auf Art 22 DSGVO. Personen haben demnach das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die rechtliche Wirkungen entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. In diesem Zusammenhang weist die DSB darauf hin, dass die Nutzung von KI zur Durchführung automatisierter Entscheidungen unter die Ausnahmetatbestände des Art 22 Abs 2 leg cit fallen muss, wie insbesondere die Einwilligung der betroffenen Person. Ansonsten muss ein Mensch diesbezüglich die Letztentscheidung treffen und er darf nicht überwiegend aufgrund des KI-Vorschlags entscheiden. Bei der Nutzung von KI-Systemen im hoheitlichen Bereich, die unter Art 22 DSGVO fallen, müssen die besonderen Anforderungen an eine

gesetzliche Grundlage nach Art 22 Abs 2 lit b und Abs 4 DSGVO erfüllt werden (siehe Informationen der DSB für Verantwortliche des öffentlichen Bereichs).

Die **Orientierungshilfe der deutschen DSK** streicht für Unternehmen klar heraus, dass Verantwortliche vor dem Einsatz von KI die **genauen Zwecke und Einsatzfelder festlegen** müssen, um einen datenschutzkonformen Betrieb sicherzustellen. Bestimmte Anwendungen von KI sind schon ex lege unzulässig, insbesondere Social Scoring und biometrische Echtzeitüberwachung öffentlicher Räume. Manche Einsatzbereiche haben generell keinen Personenbezug; in solchen Fällen unterliegt die KI-Anwendung nicht der DSGVO. Bei der Auswahl von KI-Anwendungen ist es wichtig zu prüfen, ob diese **datenschutzkonform trainiert** wurden, insbesondere ob personenbezogene Daten verwendet wurden und ob hierfür eine Rechtsgrundlage besteht.

Für jede Verarbeitung personenbezogener Daten mittels KI muss eine Rechtsgrundlage des Art 6 Abs 1 DSGVO vorliegen. Die Verarbeitung von sensiblen Daten – insbesondere von Gesundheitsdaten, biometrischen Daten etc. – erfordert zusätzlich eine Ausnahme nach Art 9 Abs 2 DSGVO. In diesem Zusammenhang ist nach Art 10 Abs 5 KI-VO die Verarbeitung sensibler Daten iSd Art 9 DSGVO erlaubt, wenn damit „Biases" in KI-Systemen entdeckt und behoben werden. Diese Verarbeitung ist selbstverständlich im **Verzeichnis für Verarbeitungstätigkeiten nach Art 30 DSGVO** aufzunehmen. Liegt kein geeigneter Rechtfertigungstatbestand vor, ist die Datenverarbeitung unzulässig, was auch den Einsatz des betreffenden KI-Systems unzulässig macht. Die Beweislast für die Einhaltung der DSGVO liegt nach Art 5 Abs 2 DSGVO beim Verantwortlichen.

Beim Einsatz von KI-Anwendungen besteht häufig ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen und dementsprechend eine Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) nach Art 35 DSGVO. Die DSK veröffentlichte eine „Muss-Liste" mit konkreten Verarbeitungstätigkeiten, für die zwingend eine DSFA durchzuführen ist. In der Orientierungshilfe empfiehlt sie Unternehmen, ihren Beschäftigten für die berufliche Nutzung von KI eigene Accounts zur Verfügung zu stellen, die ohne Verwendung von Namen und sonstigen personenbezogenen Daten einzelner Beschäftigter genutzt werden. Die Verwendung von KI-Anwendungen externer Anbieter, etwa bei Cloud-Lösungen, führt dazu, dass die externen Anbieter als Auftragsverarbeiter agieren und zwischen dem Anbieter und Verantwortlichen eine Vereinbarung gemäß Art 28 Abs 3 DSGVO geschlossen werden muss.

Die FAQ der DSB und die Orientierungshilfe der DSK veranschaulichen, dass die **DSGVO einen weitreichenden Anwendungsbereich** hat und insbesondere neue Technologien wie KI nicht davon ausgenommen sind. **Klare Regelungen zur Nutzung von KI-Anwendungen im Arbeitsalltag sind unerlässlich**, um unkontrollierte Anwendungen und Datenschutzverstöße zu vermeiden, weshalb Unternehmen und Behörden unbedingt detaillierte **interne Richtlinien und Handlungsanweisungen** implementieren sollten.

Der Europäische Datenschutzausschuss (EDSA) erarbeitet derzeit Leitlinien zum Thema KI und Datenschutz, welche eine umfangreichere Übersicht liefern sollen.

In Österreich dient die KI-Servicestelle der RTR GmbH unter https://ki.rtr.at als Ansprechpartnerin und Informationshub zum Thema KI.

---

10 Jahre „Datenschutz konkret"

KTR-Newsletter November 2024

Der MANZ Verlag lud Mitte November anlässlich des 10-jährigen Bestehens der Zeitschrift **Datenschutz konkret** zum „Datenschutz-Heurigen". Herausgeber Dr. Knyrim begrüßte die Autorinnen und Autoren und Beiratsmitglieder und präsentierte beeindruckende Zahlen zur ersten

österreichischen Fachzeitschrift für Datenschutzrecht. Etwa, dass bisher 1.228 Seiten mit 252 Fachbeiträge, 50 Checklisten, 51 Interviews (mit dem „Who is Who“ im Datenschutzrecht), 248 Entscheidungen und ca. 100 Buchbesprechungen publiziert wurden. Er wies auch darauf hin, dass die Abfragezahlen der Dako-Beiträge in der Rechtsdatenbank RDB gerade heuer den neuen Abfragerekord der letzten fünf Jahre erreichen und zuletzt am häufigsten eine Checkliste zum AI Act abgerufen wurde.

Aus dem Editorial des allerersten Heftes aus Herbst 2014 wurde bei dieser Gelegenheit auch das bis dato sehr erfolgreiche Konzept der Zeitschrift –**„kurz und knackig wie ein Sacherwürstl“** – in Erinnerung gerufen. Ein gelungener Abend zu Ehren der vielen Mitwirkenden am Erfolg der „Dako“!

Wann sind Webdesigns manipulativ?

Beitrag verfasst von Dr. Rainer Knyrim und Fabian Jelicic – KTR-Newsletter November 2024

Manipulative Webdesigns sind aus unternehmerischer und aus juristischer Sicht ein spannendes und heikles Thema. Der Europäische Datenschutzausschuss (EDSA) hat seine Leitlinien zu den sogenannten „Deceptive Design Patterns“ speziell auf Social Media-Plattformen überarbeitet und neu veröffentlicht (Guidelines 03/2022).

Die auch als „irreführenden Designs“ bekannten Manipulationstechniken zielen durch den Einsatz psychologischer Tricks darauf ab, Nutzer:innen von Apps oder Websites im Bereich der Benutzeroberfläche zu bestimmten Verhaltensweisen zu verleiten, die meist zugunsten der jeweiligen Plattformbetreiber sind, dies insbesondere in Bezug auf die Verarbeitung personenbezogener Daten. Die Leitlinien richten sich primär an Anbieter sozialer Medien und geben konkrete Empfehlungen für ein **datenschutzkonformes Design** von Benutzeroberflächen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hat zu diesen Leitlinien kürzlich sehr ausführliche und praxisnahe FAQ veröffentlicht (FAQ zu Deceptive Design Patterns).

Grundsätzlich lassen sich Deceptive Design Patterns in **sechs Kategorien** einteilen. So beschreibt „**Overloading**“ Situationen, in denen Nutzer:innen mit einer Fülle von Informationen oder Optionen konfrontiert werden, was dazu führen kann, dass sie unbeabsichtigt mehr Daten preisgeben oder einer Datenverarbeitung zustimmen, die sie sonst abgelehnt hätten. Ein Beispiel hierfür ist das „Privacy

Maze“, welches es erschwert, Datenschutzeinstellungen zu finden, weil sie hinter vielen Websiteschichten und auf verschiedenen Seiten verteilt sind.

Im Fall von „**Skipping**“ werden Benutzeroberflächen so gestaltet, dass Nutzer:innen Datenschutzaspekte übersehen oder vergessen. Dies kann etwa durch „Deceptive Snugness“ geschehen, bei dem die datenschutzfeindlichsten Einstellungen bereits vorausgewählt sind.

„**Stirring**“ nutzt Appelle oder visuelle Reize, um Entscheidungen zu beeinflussen, beispielsweise durch „Emotional Steering“, bei dem Wortwahl oder Bilder eingesetzt werden, um bestimmte Gefühle hervorzurufen und einen Steuerungseffekt auf das Verhalten der Nutzer:innen auszuüben.

Bei „**Obstructing**“ werden Hindernisse geschaffen, die es Nutzer:innen erschweren, Datenschutzeinstellungen zu ändern oder ihre Daten zu verwalten. Dies kann durch komplizierte Prozesse oder technische Barrieren geschehen. Hiervon erfasst sind bestimmte Aktionen die ins Leere führen, etwa wenn Links zu Datenschutzeinstellungen ins Nichts führen und Fehlermeldungen erzeugen (Dead End) oder wenn der Prozess zum Ändern von Einstellungen sowie zum Widerruf einer Einwilligung im Vergleich zur Erteilung der Einwilligung zu lang ist (Longer than necessary).

„**Fickle**“ bezieht sich auf inkonsistente oder verwirrende Benutzeroberflächen, die es schwierig machen, sich zurechtzufinden. Dies kann durch wechselnde Terminologie, unterschiedliche Designs oder unklare Strukturen geschehen.

Im Rahmen von „**Left in the Dark**“ werden essenzielle Informationen verborgen oder so unklar dargestellt – insbesondere durch widersprüchliche Informationen und mehrdeutige Formulierungen – , dass Nutzer:innen nicht wissen, wie ihre Daten verarbeitet werden oder welche Rechte sie haben.

Der Einsatz von Deceptive Design Patterns kann gegen mehrere Grundsätze der DSGVO verstoßen, insbesondere gegen die Prinzipien der **Fairness, Transparenz und Datenminimierung**. So können diese Patterns die Freiwilligkeit und Informiertheit der Einwilligung gemäß Art 4 Z 11 iVm Art 7 DSGVO beeinträchtigen. Zudem können vage Formulierungen und fehlende Informationen gegen die Informationspflichten nach Art 12 ff DSGVO verstoßen.

Die Leitlinien enthalten zahlreiche Best-Practice-Empfehlungen, um Deceptive Design Patterns zu vermeiden. Dazu gehört die Bereitstellung von **Shortcuts**, die direkten Zugang zu relevanten Informationen ermöglichen. Einstellungen mit gleichem Verarbeitungszweck sollten **gebündelt**, aber dennoch individuell anpassbar sein. **Kontaktinformationen** und die **Erreichbarkeit der zuständigen Aufsichtsbehörde** sollten klar und an erwarteten Stellen wie z.B. in der Datenschutzerklärung aufgeführt sein.

Der EDSA empfiehlt weiters, die **Datenschutzerklärung** übersichtlich zu gestalten, etwa durch ein Inhaltsverzeichnis. Generell erleichtern einheitliche Formulierungen und die Erklärung technischer Begriffe das Verständnis. Datenschutzrechtlich relevante Elemente sollten optisch **hervorgehoben** werden und ein Datenschutz-Onboarding nach Eröffnung eines Accounts kann Nutzer:innen helfen, von Anfang an ihre Präferenzen festzulegen. Standardmäßig sollten jedoch die datenschutzfreundlichsten Optionen aktiviert sein. Kontextbezogene Informationen, selbsterklärende URLs und ein **Formular für die Ausübung von Betroffenenrechten** tragen ebenfalls dazu bei, eine DSGVO-konforme Plattform zu betreiben. Deceptive Design Patterns können erhebliche rechtliche Konsequenzen nach sich ziehen, so hat die französische Datenschutzbehörde CNIL eine Strafe wegen der Verwendung von „Dark Patterns“ von EUR 10 Mio. gegen *Yahoo* verhängt (SAN-2023-024).

Wenngleich die Leitlinien des Europäischen Datenschutzausschusses speziell für Social Media-Plattformen verfasst wurden, empfehlen wir, auch bei der **Entwicklung von Websites und Apps** die

aufgezählten **Deceptive Design Patterns zu vermeiden** und die Empfehlungen des Datenschutzausschusses umzusetzen.

Das kann der EDSA-Datenschutz-Leitfaden für KMU (nicht)

Beitrag verfasst von Dr. Rainer Knyrim und Theodor Mach-Walter– KTR-Newsletter November 2024

Der **Leitfaden für kleine Unternehmen** des Europäischen Datenschutzausschusses (EDSA) ist seit Sommer 2024 in deutscher Übersetzung online verfügbar (https://www.edpb.europa.eu/sme-data-protection-guide/home_en).

Die Europäische Kommission definiert Unternehmen mit weniger als 250 Mitarbeiterinnen und Mitarbeitern bei einer Jahresumsatzsumme von bis zu EUR 50 Mio als KMU (kleine und mittlere Unternehmen). Das umfasst **99,6 Prozent der in Österreich tätigen Unternehmen** (https://www.bmaw.gv.at/Services/Zahlen-Daten-Fakten.html). Dementsprechend relevant ist der Leitfaden für die österreichischen Betriebe!

Der EDSA-Leitfaden besteht aus einer Webseite, auf der wesentliche Punkte, die es beim Thema Datenschutz als Unternehmen zu beachten gibt, knapp zusammengefasst sind. Wir haben uns diese angesehen:

Mit einem Video, Grafiken und Praxis-Beispielen sollen im Leitfaden auch komplexere Vorgänge wie z.B. das **Verarbeitungsverzeichnis** verständlich gemacht werden. Tatsächlich wird aber etwa genau zu diesem Punkt dann nicht viel mehr als der Inhalt des Art 30 aufgezählt und für „mehr" auf den Art 30 DSGVO und das Positionspapier der Art-29-Datenschutzgruppe in der englischen Fassung aus 2018 verlinkt.

Hilfreich ist hingegen eine Übersichtstabelle im Kapitel **„Rechte des Einzelnen respektieren"**, die zeigt, welche Betroffenenrechte bei welcher Rechtsgrundlage bestehen (https://www.edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_de).

Im Kapitel **„Datenschutzverletzungen"** gibt es neben allgemeinen Informationen zu den Melde- und Verständigungspflichten eine kurze Verlaufsgrafik, die die Frage lösen soll, ob man einen Data Breach melden muss und ob die Betroffenen zu informieren sind. Diese erklärt aber nicht die in der Praxis oft heikle Frage, wie man die Einstufung in ein hohes oder niedriges Risiko vornimmt (https://www.edpb.europa.eu/sme-data-protection-guide/data-breaches_de).

Leider auch nicht sehr hilfreich ist der Punkt „**Wie kann man eine Datenschutz-Folgenabschätzung (DSFA) durchführen?**" im Kapitel „**Seien Sie konform**" (https://www.edpb.europa.eu/sme-data-protection-guide/be-compliant_de#toc-3). Dieser enthält einen – äußerst kurzen – geführten grafischen Fragenkatalog zur Vorprüfung (sog. Schwellenwertprüfung), ob eine Datenschutz-Folgenabschätzung erforderlich ist oder nicht. Erst wenn man diesen tatsächlich „durchspielt", wird man an einer Stelle darin in einem kleinen Aufzählungspunkt darauf hingewiesen, dass es zu den Ausnahmen Regelungen der nationalen Datenschutzbehörden geben kann. Genau dies trifft beispielsweise in Österreich zu! Aufgrund der Verordnungsermächtigung in der DSGVO hat die österreichische Datenschutzbehörde zwei Verordnungen zur Datenschutz-Folgenabschätzung und den Ausnahmen von der Datenschutz-Folgenabschätzung erlassen, die bei solchen Assessments zu beachten sind. Wer sich daher mit dem reinen Textteil auf dieser Webseite begnügt, ohne den Fragenkatalog „durchzuspielen", stößt nicht auf die Information zu diesen Regelungen und wird **womöglich zu einem falschen Ergebnis** gelangen. Man würde sich hier vom EDSA, der sich immerhin aus den europäischen Datenschutzbehörden zusammensetzt, auch eine Sammlung aller nationalen

Verordnungen zur Datenschutz-Folgenabschätzung erwarten. Eine solche wäre gerade für kleine Unternehmen sehr hilfreich und fehlt leider.

Der Leitfaden des EDSA bringt an einigen wenigen Stellen einen Mehrwert, gibt aber oft nur den Text der DSGVO in anderen Worten wieder. In Summe ist er eher enttäuschend und **nur mit Vorsicht zu nutzen** und kann gerade bei KMU – wie auch in Unternehmen oder Organisationen mit geringen Ressourcen oder mangelnder rechtlicher Expertise im Datenschutz – zu einem falschen Gefühl der Einfachheit und Sicherheit führen. Tatsächlich ist die **DSGVO in der Praxis nicht so einfach zu handhaben**, wie der Leitfaden zu vermitteln versucht. Er ersetzt daher nicht die gründliche eigene Befassung mit der DSGVO!

---

200 Vorträge zum Datenschutz!

KTR-Newsletter November 2024

Für über 200 gehaltene Vorträge, über 260 Anmoderationen und 9 Jahre Privacy & Security (PriSec) erhielt Dr. Rainer Knyrim von Moritz Mirascija, Co-Geschäftsführer von Business Circle heuer auf der PriSec in Rust einen "Pokal". Er ist aus einem Stück Weinfass aus einem Ruster Weinkeller in Rust hergestellt worden (und riecht tatsächlich nach Wein). Die Gravur weist den neuen Besitzer als „Nummer 1 im Datenschutz“ aus. Ein Ehrenplatz in unserem Besprechungszimmer wurde schnell gefunden!

„Vielen Dank für die Anerkennung! Alle 200 Mal haben Spaß gemacht und mich mit interessanten Menschen zusammengebracht, denen ich hoffentlich etwas von meinem Wissen weitergeben konnte!“

Dr. Rainer Knyrim

Unsere nächsten Vorträge, Lehrgänge und Tagungen
finden Sie laufend auf unserer Homepage unter

www.kt.at/termine.
→ Tipp: Hier gibt es immer wieder auch Zusatzinfos zu Kanzlei-Rabatten!

Schlechte IT-Sicherheit kann teuer werden! Stadt Baden muss für Datenleck Schadenersatz zahlen

Beitrag verfasst von Dr. Rainer Knyrim und Erika Gleizer – KTR-Newsletter November 2024

Das Landesgerichts Wiener Neustadt (LG Wr. Neustadt) hatte die Stadt Baden wegen eines im März 2022 aufgetretenen Datenlecks zur Zahlung von Schadenersatz verurteilt. Nun wurde berichtet, dass das Oberlandesgericht Wien (OLG Wien) das Urteil bestätigt hat. Wir haben uns diese Entscheidung, die Gegenstand eines Artikels im Standard war, näher angesehen:

Das Datenleck war im Zuge der Einführung neuer Funktionen der Baden-Card aufgetreten und betraf auch Daten zu Online-Registrierungen und Bezahlvorgängen. Obwohl noch nicht alle Konfigurationsarbeiten abgeschlossen waren, wurde die neue Lösung unter Zeitdruck bereitgestellt. Dies führte dazu, dass rund 33.000 Datensätze, einschließlich Meldedaten und Zahlungsinformationen, für mehrere Tage online zugänglich waren. Ein betroffener Bürger klagte daraufhin beim LG Wr. Neustadt auf Schadenersatz.

Das LG Wr. Neustadt hatte zwar festgestellt, dass es weder zu einem Datenmissbrauch noch zu einem Diebstahl gekommen war, aber allein die begründete Sorge vor einem möglichen Missbrauch ausreiche, um einen Anspruch auf Schadenersatz zu begründen. Das OLG Wien bestätigte diese Sichtweise und führte aus, dass **bereits „die Angst und der Stress vor einer möglichen Bloßstellung und Belästigung" für den Schadenersatzanspruch genügten**. Die Stadt Baden argumentierte, der Zugriff habe nur über eine bestimmte Website erfolgen können und die betroffenen Daten seien in öffentlichen Registern zugänglich gewesen. Das OLG Wien entschied jedoch, dass ein Nachweis des tatsächlichen Missbrauchs der Daten nicht erforderlich sei. Diese Sichtweise deckt sich mit einem Urteil des Europäischen Gerichtshofs vom 14.12.2023 (EuGH C-340/21), wonach **Unternehmen und Behörden bei Datenlecks auch ohne nachweisbaren materiellen Schaden haftbar gemacht werden können.**

Darüber hinaus stellte das OLG Wien fest, dass die Stadt Baden die **Verantwortung** für die IT-Installation der Baden-Card **nicht auf das beauftragte IT-Unternehmen abwälzen** kann. Eine Haftungsfreistellung gemäß der DSGVO sei nicht möglich, da die Stadt trotz unvollständiger Konfiguration bewusst das Risiko von Sicherheitslücken in Kauf genommen habe.

Fazit: Schlechte IT-Sicherheit kann teuer werden! Obwohl der Schadenersatz von EUR 500,00 pro Person auf den ersten Blick gering erscheinen mag, kann er sich bei einer großen Anzahl Betroffener zu erheblichen Beträgen summieren. Würden etwa in diesem Fall alle 33.000 Betroffenen Schadenersatz einklagen und EUR 500,00 zugesprochen erhalten, wären das in Summe 16,5 Millionen Euro!

Publikationen unserer Kanzlei

KTR-Newsletter November 2024

Gemäß unserem Motto „Wir schreiben selbst" haben wir auch in den letzten Monaten mehrere Beiträge veröffentlicht und arbeiten bereits an den nächsten Projekten.

VORSCHAU

Knyrim, Data Act
Anfang nächsten Jahres wird in den MANZ Sonderausgaben zu den EU-Digitalisierungsrechtsakten der Band zum Data Act erscheinen und die Serie, in der bereits die Ausgaben zu DMA, DGA und DSA verfügbar sind, ergänzen.

Bald erhältlich im MANZ Shop HIER.

UNSERE NEUEN BEITRÄGE IN FACHZEITSCHRIFTEN

Rainer Knyrim, Stephanie Briegl
NIS-2: die Anwendung im Konzern. Netz- und Informationssysteme; Cybersicherheit; Konzernbetroffenheit., Dako 4/2024, 78ff.

Nachzulesen HIER.

Rainer Knyrim
Das neue Medienprivileg des § 9 DSG. Redaktionsgeheimnis; Transparenz; Compliance-Verpflichtungen; Betroffenenrechte; Bürgerjournalismus., Dako 4/2024, 80f.

Nachzulesen HIER.

Gerald Trieb
Ein effektiver Datenschutz erfordert fortlaufende Anstrengungen und ausreichend Ressourcen. Interview mit Alma Zadić, Bundesministerin für Justiz, Dako 4/2024, 74f.

Nachzulesen HIER (RDB).

Rainer Knyrim, Stephanie Briegl
Datenzugangsansprüche im Vergleich: Datenportabilität (DSGVO) und Datenzugang (Data Act), Dako 5/2024, 102ff.

Nachzulesen HIER (RDB).

Gerald Trieb
VwGH bestätigt neue restriktive Judikatur zur Speicherdauer von Daten zur Rechtsschuldbefreiung, ZFR 8/2024, 165.

Nachzulesen HIER.

Rainer Knyrim, Stephan Varga
Beschränkungen des Informationsrechts nach IFG aufgrund der berechtigten Interessen eines Anderen, ecolex 10/2024, 832ff.

Nachzulesen HIER.

KÜRZLICH ERSCHIENEN

Knyrim (Hrsg.), Der DatKomm, Lfg. 77-84
Im September 2024 erschien die aktuelle Ergänzungslieferung des österreichischen DSGVO- und DSG-Kommentars mit den exzellenten Überarbeitungen von Mag. Ursula Illibauer, MA (Art 12-14) Mag. Viktoria Haidinger, LL.M. (Art 15-19), Dr. Andreas Zavadil (Art 51-59), Prof. Dr. Eva Souhrada-Kirchmayer (Art 78) und Mag. Marija Križanac (Art 94-99).

Erhältlich im MANZ Shop HIER.

Wir veröffentlichen unsere Publikationen bzw. Neuigkeiten dazu
auch regelmäßig auf unserer Homepage unter
https://www.kt.at/publikationen/.

Knyrim Trieb Rechtsanwälte OG

Mariahilfer Straße 89a, A-1060 Wien, T: +43 1 909 30 70, F: +43 1 909 36 39
E: kt@kt.at, W: www.kt.at
FN 462250f, HG Wien