Secur-Data Betriebsberatungs-Ges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at
Offenlegung gem. MedienG: www.secur-data.at/impressum

DSG-Info-Service

Mai 2023 Ausgabe Nr. 106

Liebe Leserinnen und Leser,

Jubiläen und neue Technologien prägen das Datenschutzjahr im Mai:

Am 25. Mai 2023 feiert die DSGVO ihren fünften Geburtstag, unter intensiver medialer Begleitmusik und zahlreichen Fachevents hybrid und vor Ort. So findet etwa von 24. bis 26. Mai bereits zum 16. Mal die internationale Konferenz CPDP2023 (Computers, Privacy and Data Protection) in Brüssel statt. Auch die Wirtschaftskammer lässt am 25. Mai um 17:00 unter dem Titel „5 Jahre DSGVO in Europa – Datenschutz-Vorbild oder Digitalisierungsbremse?" zum Thema diskutieren. Hochkarätig wird es auch bei der Tagung des Privacy Rings im Königlichen Pferdestall in Hannover[1]: Der Event „#DSA, #DMA, #DGA, #DataAct – im Normendschungel der EU" wirft am 25. und 26. Mai (Teilnahme vor Ort oder online) einen kritischen Blick auf die neuen EU-Acts (mit Livepodcast, Workshops und interessantem Rahmenprogramm).

Die rasante Entwicklung von KI und Anwendungen wie ChatGPT halten die Datenschutzwelt derzeit in Atem. Kaum ein Tag, wo nicht ein neuer Entwicklungssprung vermeldet und neue Chancen oder Gefahren thematisiert und diskutiert werden. Finden Sie dazu eine ausführliche Analyse gleich zu Beginn unseres Mai-Newsletters. Auf ein (zumindest temporäres) „Happy End" warten wir auch beim Dauerthema Datentransfer in die USA, der EU-Angemessenheitsbeschluss wird ja für kommenden Sommer avisiert. Dass nun auch die Amerikaner ihre Daten vor europäischen Zugriffen schützen wollen, gibt der Diskussion einen interessanten Spin. Lesen Sie dazu unsere Analyse, zusammen mit einem kurzen Streiflicht auf den Status Quo des US-Datenschutzrechts.

Nicht minder intensiv läuft die Diskussion um die EuGH-Entscheidung zum Artikel 15 DSGVO, wonach dieser den Verantwortlichen zur Nennung der konkreten Empfänger an den Betroffenen verpflichtet. Wie Unternehmen diesen Mehraufwand stemmen können – auch dazu in unserem Newsletter ein kurzer Kommentar. Zudem entschied der EuGH vor kurzem zum ersten Mal über die Voraussetzungen der Zuerkennung von Schadenersatz für immateriellen Schaden (Art 82 DSGV0), ebenso präzisierte das Gericht den notwendigen Umfang einer „Kopie". Finden Sie auch dazu eine kurze rechtliche Einschätzung.

Last not least unser bewährtes „Ranking" der Datenschutz-Bußgelder sowie ein Aviso zum Secur-Data-Praxisseminar im Herbst mit den ersten Zwischenergebnissen zum HinweisgeberInnenschutzgesetz – und wer weiß, vielleicht klappt's bis dahin ja auch schon mit dem transatlantischen Datenschutzrahmen?

Spannende Lektüre wünscht Ihre

Mag. Judith Leschanz

[1] https://kurzelinks.de/z89x

1. EU-Regelung für Künstliche Intelligenz nimmt Gestalt an

OpenAI hat mit ChatGPT eine KI-Plattform entwickelt, die menschenähnliche Konversationen führen kann. Sie wird in Kundenservice, Bildung und Unterhaltung eingesetzt und ist eine der fortschrittlichsten KI-Plattformen auf dem Markt. Unternehmen und Organisationen nutzen ChatGPT weltweit, um ihre Kundenerfahrung zu verbessern und Prozesse zu automatisieren.

Hätten Sie erkannt, dass diese Sätze von einer Künstlichen Intelligenz (KI) und nicht von einem Menschen verfasst wurden? Genau diese Möglichkeiten beeindrucken und verstören seit dem Start von ChatGPT im November 2022 vor allem den Wirtschafts- und Bildungssektor. Mit der Öffnung von künstlicher Intelligenz für die breite Masse der Gesellschaft gehen aber auch Gefahren wie zB Urheberrechtsverletzungen und Diskriminierung einher.

Ähnliche Bedenken hatten die Europäische Kommission schon im April 2021 dazu veranlasst, das weltweit erste Regelwerk für Künstliche Intelligenz, den AI-Act,[2] zu initiieren. Dieser verfolgt einen risikobasierten Ansatz, der je nach potenziellen Gefahren und Fähigkeiten der konkreten Anwendung Auflagen und Verbote vorsieht. Außerdem sollen Nutzer, die von KI-Anwendungen geschädigt wurden, einen außervertraglichen Schadenersatzanspruch gegenüber den Betreibern und Herstellern erhalten. Ähnlich wie in der DSGVO sind auch im AI-Act hohe Bußgelder (bis zu EUR 30 Mio. bzw. bis zu 6 % des weltweiten Jahresumsatzes) für Verstöße vorgesehen.

Der Gesetzesvorschlag der Kommission wurde in den vergangenen Monaten von den Ausschüssen des Europäischen Parlaments (*IMCO* und *LIBE*)[3] ausführlich diskutiert. Umstritten war beispielsweise die Regulierung polizeilicher Befugnisse im Zusammenhang mit KI-Systemen, das sogenannte „predictive policing". Das Verbot von biometrischer Echtzeit-Datenerfassung im öffentlichen Raum fand breiten Konsens, jedoch wurden immer wieder Ausnahmetatbestände, zum Beispiel zur Wahrung der nationalen Sicherheit, ins Spiel gebracht.

Zuletzt wurden Forderungen in Bezug auf sogenannte generative KI-Modelle bekannt. Anbieter solcher Dienste sollen zum Schutz der Urheber angeben, ob urheberrechtlich geschütztes Material für das Trainieren der KI benutzt worden ist. Nun hat man sich Ende April auf eine Endfassung geeinigt, sodass der AI-Act in den nächsten Verfahrensabschnitt, den Trilog, verabschiedet werden kann.

Der österreichische Weg

In Österreich kritisierte Digitalstaatssekretär Florian Tursky den schleppenden Fortschritt der EU-Verordnung. Er kündigt für das heurige Jahr noch eine nationale gesetzliche Regulierung für Künstliche Intelligenz an. Außerdem soll ab 2024 eine eigene KI-Behörde installiert werden, die Aufgaben wie die Einstufung von Algorithmen nach Gefährdungsgrad und das Auszeichnen vertrauenswürdiger KI mit eigenem Gütesiegel wahrnimmt. Ob Wien oder Brüssel als Erster verbindliche KI-Regulierungen erlässt, ist noch offen. Wir halten Sie auf dem Laufenden!

[2] https://kurzelinks.de/71wv

[3] Internal Market and Consumer Protection; Civil Liberties, Justice and Home Affairs

Italien hebt ChatGPT-Sperre wieder auf

Die italienische Datenschutzbehörde GPDP (Garante per la Protezione dei Dati Personali, „Garante della privacy“) hatte am 31. März den KI-Dienst ChatGPT mit sofortiger Wirkung im gesamten Land sperren lassen.[4] Grund für die Sperre waren unter anderem der fehlende Jugendschutz und der Verdacht, dass personenbezogene Daten durch den US-Betreiber OpenAI unrechtmäßig verarbeitet werden. Nur knapp einen Monat später wurde die Sperre wieder aufgehoben,[5] nachdem OpenAI auf sämtliche datenschutzrechtlichen Forderungen der GPDP eingegangen ist.

Europäische ChatGPT-Nutzer können nunmehr die Verarbeitung ihrer persönlichen Daten zu KI-Trainingszwecken untersagen und ihre gespeicherten Eingaben beauskunften und löschen lassen. Auch die Datenschutzerklärung ist nun bereits vor der Registrierung zugänglich und nicht erst nach dem erfolgten Login. Die Aufsichtsbehörde begrüßte zwar die neuen Maßnahmen von OpenAI, fordert aber noch einen Altersfilter und Informationen über die Opt-Out-Möglichkeit.

Nicht so streng sehen unsere deutschen Nachbarn in Schleswig-Holstein die Nutzung von ChatGPT. Laut Digitalisierungsminister Dirk Schrödter soll der KI-Dienst in der öffentlichen Verwaltung des norddeutschen Bundeslandes eingesetzt werden und für eine effizientere und automatisierte Arbeitsweise sorgen. Anwendungsfälle könnten vorbereitende Recherchearbeiten für Reden, Sachverhaltsdarstellungen oder Aktenvermerke sein.

Wenig begeistert zeigte sich daraufhin Marit Hansen, Landesdatenschützerin von Schleswig-Holstein. Sie weist auf die möglichen Risiken des KI-Einsatzes und die fehlende Rechtsgrundlage für die Verarbeitung personenbezogener Daten der Bürger*innen hin.

2. Politisches Gerangel um Datentransfer in die USA: EU-Überwachungspraktiken im Radar des US-Justizministeriums

Kennen wir dies nicht in die andere Richtung? Viele Jahre lang hatte Brüssel die USA wegen ihres leichtfertigen Umgangs mit europäischen Daten kritisiert und Washington kein angemessenes datenschutzrechtliches Schutzniveau zugestanden. Die Folge waren zähe Verhandlungen über die Gewährung von ausreichendem Rechtsschutz beim Datentransfer in die USA. Im Rahmen der abschließenden Verhandlungen über das TADPF (Trans-Atlantic Data Protection Framework) hinterfragt das US-Justizministerium nunmehr seinerseits Überwachungspraktiken der EU-Mitgliedstaaten.

Nachgefragt wird etwa, ob Länder wie Ungarn oder auch Frankreich valide Rechtsmittel zur Verfügung stellen, mit denen sich Nicht-EU-Bürger gegen (überschießende) Datensammlungen der nationalen Sicherheitsbehörden wehren können. Außerdem fordern die Vereinigten Staaten Informationen, wer die Datensammlungen der europäischen Staaten kontrolliert und welche rechtlichen Grenzen einzuhalten sind.

Der US-Justizminister sieht diese als Voraussetzung, ein eigenes System wirksamer Rechtsbehelfe fertigzustellen. Dieser Mechanismus soll es europäischen Bürgern ermöglichen, bei

[4] Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di... - Garante Privacy: https://kurzelinks.de/3dr6

[5] ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più... - Garante Privacy: https://kurzelinks.de/tzus

Datenschutzverstößen in einem eigenen Verfahren Klage gegen amerikanische nationale Sicherheitsbehörden erheben zu können – die letzte Hürde zum ersehnten Brüsseler Angemessenheitsbeschluss. US-Beamten missfällt die Einseitigkeit der Diskussion schon lange, sie empfinden es als ungerechtfertigt, dass nur die US-Seite für Datenspionage kritisiert wird. Deshalb möchten die USA nunmehr den Europäern den Spiegel vorhalten und verlangen ihrerseits Auskunft über Spionagepraktiken.

Beobachter sehen in den wechselseitigen Unfreundlichkeiten mehr ein politisches Geplänkel als eine ernsthafte Gefährdung des transatlantischen Abkommens zum Datenaustausch, fällt doch die Datenüberwachung der Sicherheitsbehörden unter die Zuständigkeit der einzelnen Mitgliedsländer und nicht – wie das TADPF – die der Kommission. Der Pakt wird voraussichtlich im Sommer 2023 unterzeichnet.

Datenschutz auf amerikanisch – Ein Überblick

Anders als in Österreich oder Deutschland gibt es in den USA kein allgemeines bundesweites Datenschutzgesetz, sondern jeweils eigene branchenspezifische Datenschutzgesetze für einzelne Bereiche wie etwa Wirtschaft und Handel oder den Finanzsektor. Der Schutz personenbezogener Daten wird im Gegensatz zu Europa nicht als Grundrecht qualifiziert, sondern lediglich als Teil des Verbraucherschutzes. Einzelne US-Bundesstaaten haben jedoch umfassende Datenschutzgesetze verabschiedet, zuletzt etwa Montana und Tennessee. Davor hatten – nach Connecticut, Utah, Virginia, Colorado und Kalifornien – Indiana und Iowa ihre Data Protection Acts präsentiert.

Sieht man sich die einzelnen Acts im Detail an, so kann man durchaus zu dem Schluss kommen, dass auch US-Staaten den Regelungsbedarf für datenschutzrechtliche Fragestellungen ernst nehmen. So gilt etwa der Montana Consumer Data Privacy Act (MCDPA) für Unternehmen, die in Montana geschäftlich tätig sind, personenbezogene Daten von mehr als 50.000 Verbrauchern kontrollieren und mehr als 25 % ihrer Bruttoeinnahmen aus dem Verkauf dieser Daten erwirtschaften.

Personenbezogene Daten werden – wie in der EU – als Informationen definiert, die mit einer identifizierten oder identifizierbaren Person verknüpft sind. Auch den Begriff der „sensiblen Daten“ kennt man in den erwähnten US-Staaten, darunter fallen etwa Rasse/ethnische Herkunft, Religion, Gesundheitsdiagnosen, Sexualleben und sexuelle Orientierung, die Staatsbürgerschaft, der Einwanderungsstatus und genetische oder biometrische Informationen einer betroffenen Person. Sensible Daten dürfen nicht verarbeitet werden, ohne dass die Zustimmung des Verbrauchers eingeholt wurde. Die Unternehmen müssen den Konsumenten außerdem eine Reihe von „Standardrechten“ zugestehen, darunter das Recht auf Ablehnung des Verkaufs personenbezogener Daten, das Recht auf Löschung, Zugang, Berichtigung und Widerspruch, das Recht auf Einwilligung in Werbung und gezieltes Marketing sowie das Recht auf Datenübertragbarkeit.

Die für die Verarbeitung Verantwortlichen sind außerdem zu Datenminimierung, Verhältnismäßigkeit, angemessenen Sicherheitsmaßnahmen und Transparenz verpflichtet – Grundsätze, die auch für die DSGVO zentral sind. Schade, dass der Act nur US-Bürger schützt und nicht auch europäische Betroffene. Aber immerhin, einzelne Bundesstaaten sind auf einem guten Weg – der Weg zu einem bundesweiten Gesetz ist aber noch weit.

3. EuGH-Urteil im „Post-Datenskandal“: Mehr Aufwand durch Pflicht zur Benennung konkreter Empfänger

Das Urteil vom Jänner 2023 hatte in der Datenschutz-Community für Aufsehen gesorgt: Im Zuge eines Auskunftsbegehrens gegen die Österreichische Post AG als Verantwortliche wegen der Weitergabe personenbezogener Daten an Geschäftskunden zu Marketingzwecken hatte sich das Unternehmen geweigert, konkrete Empfänger*innen zu nennen – zu Unrecht, wie der EuGH befand: Der Verantwortliche habe die Verpflichtung, der betroffenen Person die Identität der Empfänger mitzuteilen, eine Auflistung der Kategorien von Empfängern sei nicht ausreichend *(siehe auch unseren Bericht in DSG-Info 104/2023).*

Für Verantwortliche insbesondere in größeren Unternehmen bedeutet diese Auslegung des Art. 15 Abs. 1 lit. c DSGVO erheblichen Mehraufwand, sowohl beim Monitoring ihres Datenschutzmanagements, der Einholung von Informationen und der Beantwortung von Auskunftsersuchen wie auch bei der Dokumentation der Auftragsverarbeiter und etwaiger Unterauftragnehmer. Eine Ausnahme von der Verpflichtung, konkrete Empfänger und nicht bloß Empfängerkategorien zu nennen, gesteht der EuGH nur in zwei Fällen zu: Wenn es dem Verantwortlichen nicht möglich ist, die Empfänger zu identifizieren oder wenn das Auskunftsbegehren der betroffenen Person offenkundig unbegründet oder exzessiv im Sinne von Art. 12 Abs. 5 DSGVO ist.

Aus datenschutzrechtlicher Sicht ist angesichts der EUGH-Entscheidung dringend eine Anpassung der unternehmensinternen Verarbeitungsprozesse zu empfehlen. So sollte für den Verantwortlichen ersichtlich sein, welche konkreten Empfänger bei einer bestimmten Verarbeitungstätigkeit im Zusammenhang mit bestimmten betroffenen Personen eine Rolle spielen. Auch die entsprechende Dokumentation der konkreten Empfänger etwa im Verarbeitungsverzeichnis kann dabei hilfreich sein. Außerdem sollte es möglich sein, etwaige Subauftragnehmer zeitnah zu benennen.

Im Ergebnis, EuGH sei Dank: Mehr Aufwand, mehr Arbeit, mehr Dokumentationspflichten!

4. Wichtige EuGH-Entscheidung zum Schadenersatz

Zwei brisante EuGH-Entscheidungen mit Österreichbezug: Immaterieller Schadenersatz: Kein Schadenersatz ohne Schaden; § 15-Auskunftsrecht: Was genau muss eine Kopie umfassen?

Gleich dreimal entschied der EuGH Anfang Mai zum Thema Datenschutz: In der mit Spannung erwarteten Entscheidung in der Rechtssache *C-300/21 – Österreichische Post*[6] urteilte das Gericht über die Voraussetzungen und die Berechnung von Schadenersatz auf Grundlage von Art. 82 DSGVO. Im Verfahren *C-487/21 Österreichische Datenschutzbehörde gegen CRIF*[7] sprach der EuGH über das Recht auf Kopie nach Art. 15 Abs. 3 S. 1 ab. In der dritten Causa, *C-60/22 – Bundesrepublik Deutschland (Boîte électronique judiciaire)*[8] entschied der Gerichtshof schließlich, dass zwischen der Rechtsgrundlage für eine Datenverarbeitung

[6] https://kurzelinks.de/0izf
[7] https://kurzelinks.de/s7nk
[8] https://kurzelinks.de/6fl5

einerseits und „begleitenden“ Compliance-Pflichten nach der DSGVO differenziert werden muss.

Insbesondere dem Urteil hinsichtlich des Zuspruchs von Schadenersatz nach Art. 82 DSGVO war ein intensiver Diskussionsprozess in Lehre und Praxis vorangegangen: Einem Kunden war von der Österreichischen Post AG aufgrund einer KI-basierten Informationsanalyse eine bestimmte parteipolitische Affinität zugeordnet worden. Der Betroffene begehrte daraufhin Ersatz des immateriellen Schadens i.H.v. EUR 1.000,00 mit der Begründung, ein großes *Ärgernis* und einen *Vertrauensverlust* sowie ein *Gefühl der Bloßstellung* verspürt zu haben.

Der Gerichtshof stellt nunmehr klar: Ein bloßer Verstoß gegen die DSGVO begründet keinen Schadenersatz, ein Ersatzanspruch ist lediglich dann gegeben, wenn tatsächlich ein Schaden entstanden ist. Hinsichtlich der Höhe des Schadenersatzanspruchs verweist das Gericht auf die nationalen Vorschriften der Mitgliedsstaaten, wobei die unionsrechtlichen Grundsätze der Äquivalenz und Effektivität zu beachten seien. Eine Erheblichkeitsgrenze für die Geltendmachung von Schadenersatz verneinte der EuGH jedoch. Ein solches Erfordernis werde in der DSGVO nicht erwähnt und stünde auch im Widerspruch zum vom europäischen Gesetzgeber gewählten weiten Verständnis des Schadenbegriffs.

Von Konsumentenschützern wird die Entscheidung begrüßt, da sie den Weg zur Durchsetzung der Ansprüche Betroffener freimacht. Zehn weitere Vorabentscheidungsverfahren sind beim EuGH derzeit noch zur Thematik anhängig.

Umstrittene EuGH-Entscheidung:
Was genau umfasst das „Recht auf Kopie“?

In einem weiteren Urteil mit österreichischer Vorgeschichte entschied der EuGH über das Recht auf Kopie aus Art. 15 Abs. 3 DSGVO. Gegenstand des ursprünglichen Verfahrens war ein Auskunftsbegehren eines Betroffenen nach Art. 15 DSGVO gegen die Kreditauskunftei CRIF. Mit dem Erhalt einer Liste seiner personenbezogenen Daten in aggregierter Form sah der Betroffene seinen Anspruch nicht ausreichend erfüllt, vielmehr seien ihm eine Kopie sämtlicher seine Daten enthaltender Dokumente wie E-Mails und Auszüge aus Datenbanken etc. zu übermitteln. Der Fall landete vor dem EuGH mit der Fragestellung, was der Begriff „Informationen“ in Art. 15 Abs. 3 S. 3 DSGVO genau umfasst.

Dazu urteilte das Gericht, dass das Recht dahingehend auszulegen ist, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller personenbezogenen Daten zur Verfügung gestellt wird, wenn dies unerlässlich ist, um ihr die wirksame Ausübung der durch die DSGVO verliehenen Rechte zu ermöglichen. Im Übrigen beziehe sich der Begriff „Kopie“ nicht auf ein Dokument als solches, sondern auf die personenbezogenen Daten, die es enthält und die vollständig sein müssen. Die Kopie muss daher alle personenbezogenen Daten enthalten, die Gegenstand der Verarbeitung sind.

Zudem stellte der EuGH klar, dass sich der Begriff „Informationen“ in Art. 15 Abs. 3 S. 3 DSGVO ausschließlich auf die personenbezogenen Daten bezieht, die der Verantwortliche gemäß Art. 15 Abs. 3 S. 1 DSGVO in Form einer Kopie zur Verfügung stellen muss.

Ob damit alle Fragen abschließend geklärt wurden, bleibt abzuwarten.

5. Top 3 DSGVO-Bußgelder im April 2023

14,5 Millionen Euro Bußgeld für TikTok

Wieder einmal wird die chinesische Social-Media-Plattform zur Kassa gebeten. Diesmal hat die britische Aufsichtsbehörde Information Commissioner's Office (ICO) das saftige Bußgeld in Höhe von 12,7 Millionen Pfund (EUR 14,5 Millionen) gegen die TikTok Information Technologies UK Limited verhängt. Hintergrund: Im Jahr 2020 hatten sich 1,4 Millionen Kinder unter 13 Jahren auf der Plattform entgegen TikToks eigenen Regeln registriert und ein Benutzerkonto eröffnet. Das Unternehmen habe es jedoch verabsäumt, angemessene Alterskontrollen zur Identifizierung minderjähriger Kinder zu implementieren. Dadurch wurden personenbezogene Daten von Kindern ohne Einwilligung deren Eltern von TikTok verarbeitet und damit das geltende Datenschutzrecht, Art. 8 DSGVO, verletzt.

Grenzüberschreitende Kooperation gegen skandinavische Fitness-Kette

Dass mit den Betroffenenrechte der DSGVO nicht zu spaßen ist, musste Skandinaviens größte Fitnesskette SATS auf die harte Tour lernen. KundInnen hatten sich bei den Aufsichtsbehörden über die mangelhafte Umsetzung ihrer Betroffenenrechte beschwert und so eine grenzüberschreitende Zusammenarbeit der Datenschützer veranlasst, welche mit einem empfindlichen Bußgeld in der Höhe von EUR 858.590 für SATS endete. Zu den Verletzungen gehörten vor allem die Nicht- bzw. nicht fristgerechte Beantwortung von Betroffenenanfragen und die fehlerhafte Rechtsgrundlage, auf der die Datenverarbeitungen unternommen wurden. So rechtfertigte SATS zum Beispiel die Verarbeitung von Trainingsverlaufsdaten mit der erforderlichen Vertragserfüllung.

Das Herzstück der DSGVO ist der Schutz und die Gewährleistung der Betroffenenrechte. Dementsprechend fallen auch die verhängten Bußgelder aus.

Gut gemeint ist nicht gut gemacht

Die italienische Datenschutzbehörde „Garante" strafte die Gesundheitsbehörde der süditalienischen Stadt Bari (Azienda sanitaria locale di Bari) mit einem Bußgeld in der Höhe von EUR 50.000 ab. Die Behörde hatte im Feedbackbereich ihrer Homepage Informationen über den Gesundheitszustand von Betroffenen, die sich aus Briefen, Dankesschreiben und E-Mails an die Gesundheitsbehörde ergaben, veröffentlicht.

Zwar wurden die im Schreiben enthaltenen personenbezogenen Daten mit Filzstift geschwärzt, jedoch waren einige Informationen nach der Veröffentlichung noch immer erkennbar. Die Datenschutzbehörde stellte fest, dass das manuelle Schwärzen kein geeignetes Mittel zur Anonymisierung von personenbezogenen Daten sei. Hier können wir nur sagen: Gut gemeint ist nicht gleich gut gemacht.

6. Internes

Von 24. Mai bis 26. Mai findet bereits zum 16. Mal die internationale Konferenz CPDP2023[9] (Computers, Privacy and Data Protection) in Brüssel statt. Da heuer die DSGVO ihren fünften Geburtstag feiert, werden besonders aktuelle Datenschutzfragen im Fokus stehen. Secur-Data Geschäftsführerin Mag. Judith Leschanz wird als Expertin zum Thema „Neue EU-Acts und die Rolle der Datenschutzbeauftragten“ an einer der Podiumsdiskussionen teilnehmen.

In der Februar-Ausgabe der Fachzeitschrift „Datenschutz Konkret“ finden Sie eine ausführliche und vor allem praxisrelevante Checkliste zur Umsetzung des HinweisgeberInnenschutzgesetzes (HSchG) von Prof. KommR Hans-Jürgen Pollirer. Sie behandelt alle relevanten gesetzlichen Regelungen zu Anwendungsbereich, Umsetzungsfristen, Dokumentationspflichten, Informationssicherheit und Sanktionen.

Secur-Data Praxisseminar revisited:

Das neue HinweisgeberInnenschutzgesetz (HSchG) sowie eine ganze Reihe neuer EU-Acts standen bei der jüngsten Ausgabe der bewährten Praxis-Updates zum Datenschutz im März im Zentrum der Diskussion

Viel Interesse und anregende Diskussionen gab es beim zweitägigen Secur-Data Datenschutz-Follow-Up im Hilton Plaza, bringt doch 2023 einige wichtige datenschutzrechtliche Neuerungen, sowohl national als auch auf EU-Ebene. Ein Top-Thema war das jüngst erlassene HinweisgeberInnenschutzgesetz (HSchG). Mit einer Übersicht der To-Dos für betroffene Unternehmen und aller wichtigen Fristen und Prozesse erwies sich das Secur-Data Praxisseminar einmal mehr als optimales Format, um aktuelle Fragestellungen mit Expert*innen aus IT und Recht zu diskutieren und die praktische Umsetzung unterschiedlichster Anwendungsfälle zu screenen.

Dies gilt insbesondere auch für die neuen EU-Acts betreffend KI und Big Data sowie den „Dauerbrenner“ des rechtskonformen Datentransfers in die USA. Hier wartet man ja voller Ungeduld auf den entsprechenden EU-Angemessenheitsbeschluss. Dieser und eine erste Umsetzung der geforderten Whistleblowing-Meldekanäle sollten beim nächsten Secur-Data-Seminar im Oktober bereits vorliegen.

Mag. Judith Leschanz, Mag. Sylvia Metenczuk, Menas Saweha, Prof. KommR Hans-Jürgen Pollirer

Save the Date:

Nächstes Seminar: 23. und 24. Oktober 2023, Vienna Hilton Plaza

Wir freuen uns auf Ihre Anmeldung!

[9] https://www.cpdpconferences.org/schedule