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

März 2023 Ausgabe Nr. 105

Liebe Leserinnen und Leser!

Wir hoffen, Sie sind aktiv und erfolgreich ins neue Geschäftsjahr gestartet!

Das Datenschutzjahr 2023 verspricht spannend zu werden. Mit Beschluss des lang erwarteten HinweisgeberInnenschutzgesetzes sind viele Unternehmen gefordert, ihre Whistleblowing-Kanäle anzupassen. Allen politischen Kontroversen zum Trotz liegt das Regelwerk nunmehr vor und muss auch umgesetzt werden. Besuchen Sie dazu auch unser Praxisseminar am 28. und 29. März 2023 im Vienna Hilton Plaza für ein Update zu den wichtigsten aktuellen Rechtsänderungen und wie Sie diese zeit- und kostensparend in Ihre Unternehmensprozesse implementieren.

Weiterhin schwierig zeigt sich die Lage beim Datentransfer in die USA. Das Trans Atlantic Data Privacy Framework (TADPF) harrt ja des EU-Angemessenheitsbeschlusses, wird aber bereits im Vorfeld nicht nur von Datenschutzverbänden kritisiert. So sprach sich auch jüngst das nicht unbedeutende LIBE Committee (Committee on Civil Liberties, Justice and Home Affairs) des Europäischen Parlaments gegen das Abkommen aus, mit der Empfehlung an die Europäische Kommission, das TADPF-Vertragswerk als datenschutzrechtlich nicht angemessen zu beurteilen. Es bleibt spannend …

In bewährter Weise haben wir auch jüngste Gerichtsentscheidungen für Sie kommentiert, etwa zu den Themen Abrufbarkeit des Datenschutzbeauftragten und zur Klagebefugnis von Verbraucherschutzverbänden. Last, but not least die Top-3 Bußgelder der letzten beiden Monate.

Wir wünschen eine angenehme Lektüre und freuen uns, Sie bei unserem Praxisseminar am 28. und 29. März persönlich begrüßen zu dürfen!

Mag. Judith Leschanz
Geschäftsführung

1. HinweisgeberInnenschutzgesetz (HSchG) beschlossen – To-Dos für Unternehmen

Am 1. Februar 2023 wurde das neue HinweisgeberInnenschutzgesetz (HSchG) im Nationalrat beschlossen, am 16. Februar gab auch der Bundesrat sein Okay, mit 25. Februar ist es in Kraft getreten. Von der Regierungskoalition als großer Wurf verkauft, stand das neue Regelwerk schon zuvor in der Kritik. Der sachliche Geltungsbereich sei zu schmal, würden doch

Rechtsverletzungen wie Mobbing, Diskriminierung, Betrug oder Untreue nicht erfasst. Auch hinsichtlich der Beweislastumkehr sei die EU-Whistleblowing-Richtlinie nur teilweise umgesetzt worden. Die Befürworter hingegen sehen das HSchG als wichtigen Schritt zur Korruptionsprävention, umfasst es doch immerhin auch die Tatbestände der §§ 302-309 StGB.

Konkret schützt das neue Regelwerk Hinweisgeber*innen, die im privaten oder öffentlichen Sektor tätig sind oder waren. Unternehmen ab 50 Mitarbeiter*innen (Headcount) werden verpflichtet, Meldekanäle für Hinweise in schriftlicher oder mündlicher Form einzurichten. Für juristische Personen in den Bereichen Finanzdienstleistungen, Verhinderung von Geldwäsche und Terrorismusfinanzierung, Verkehrssicherheit und Umweltschutz gilt die Verpflichtung unabhängig von der Anzahl der Mitarbeiter*innen.

Neben der Bereitstellung vertrauenswürdiger Kommunikationswege müssen die Verantwortlichen auch umfangreiche Dokumentationspflichten erfüllen. Bei Nichteinhaltung drohen Verwaltungsstrafen zwischen EUR 20.000 und 40.000. Insbesondere der arbeitsrechtliche Schutz der Hinweisgeber*innen ist umfangreich geregelt, so dürfen dem Whistleblower als Folge seines Hinweises keine Vergeltungsmaßnahmen drohen. Aber auch dem Spannungsfeld zwischen HSchG und Datenschutz hat sich der Gesetzgeber explizit gewidmet: Betroffenenrechte kommen nicht zur Anwendung, wenn dies für die Zwecke des HschG erforderlich ist, und auch die Löschthematik wird behandelt.

Beim (komplexen) Datentransfer im Konzern muss intern geprüft werden, in welchem Umfang personenbezogene Daten zum Zweck der Bearbeitung von Meldungen weitergeleitet werden müssen.

Für die Umsetzung des HSchG hat der Gesetzgeber zwei Fristen vorgesehen: Unternehmen ab 250 Mitarbeiter*innen haben ab Inkrafttreten sechs Monate Zeit, die Verpflichtungen zu erfüllen, für Unternehmen ab 50 Mitarbeiter*innen endet die Frist mit 17. Dezember 2023.

Besuchen Sie dazu unser Praxisseminar am 28. und 29. März im Hilton Vienna Plaza!

2. Update zum Datentransfer in die USA: Es bleibt schwierig

Eher „Bad News“ gibt es bezüglich des Umsetzungsstandes des geplanten Trans Atlantic Data Privacy Frameworks (TADPF) zum rechtskonformen Datentransfer in die USA. Hier ist ja im Moment die EU am Zug, einen Angemessenheitsbeschluss zu fällen.

Das LIBE Committee des Europäischen Parlaments (Ausschuss für bürgerliche Freiheiten, Justiz und Inneres) hat jüngst dazu den Entwurf einer Stellungnahme veröffentlicht, in dem es das TADPF vehement kritisiert und der Kommission nahelegt, keinen Angemessenheitsbeschluss zu treffen (*„urges the Commission not to adopt the adequacy finding“).* Zentrale Begriffe wie die Verhältnismäßigkeit würden im US-Recht anders als nach der DSGVO ausgelegt, auch gelte Joe Bidens‘ Executive Order (Grundlage des TADPF) nicht für Daten, die US-Behörden auf andere Weise erlangen, z.B. über den US CLOUD Act, durch freiwillige Bekanntgabe oder durch Datenkauf. Auch sei der Rechtsschutz unvollkommen und schließlich: die USA habe immer noch kein Bundes-Datenschutzgesetz.

Also doch kein Angemessenheitsbeschluss der EU in absehbarer Zeit? In der Bundessparte Information und Consulting der WKO sieht man die Lage etwas entspannter. Die LIBE sei nicht der einzige wichtige Player auf EU-Ebene: Angemessenheitsbeschlüsse der EK seien im Komitologieverfahren durchzuführen. Hierfür zustimmungs- (bzw. ablehnungs-) berechtigt

ist der Ausschuss für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (2018), der auch Vertreter*innen aus den Mitgliedstaaten umfasst. Stimmt dieses Gremium allerdings auch gegen den Angemessenheitsbeschluss, wäre nur noch der – unwahrscheinliche – Weg zum Berufungsausschuss möglich.

3. Abberufbarkeit und Interessenskonflikt beim Datenschutzbeauftragten (Art. 38 DSGVO): EuGH bleibt vage

Eher unbestimmt blieb der EuGH vor kurzem in seiner Entscheidung zur Frage der rechtskonformen Abberufung eines Datenschutzbeauftragten sowie in seinen Ausführungen, wann ein Interessenskonflikt im Sinne des Art. 38 DSGVO vorliege.

Im Vorabentscheidungsverfahren C-453/21 hatte das Gericht bezüglich der Abberufung eines bei der X-FAB Dresden GmbH & Co. KG beschäftigten Datenschutzbeauftragten zu entscheiden: Der Beschäftigte war gleichzeitig Datenschutzbeauftragter und Betriebsratsvorsitzender, was das Unternehmen für unvereinbar hielt und als legitimen „wichtigen Grund" sah, den Arbeitnehmer zu kündigen. Der EuGH stellt nunmehr klar, dass Art. 38 Abs. 3 Satz 2 der DSGVO einer nationalen Regelung nicht entgegensteht, nach der ein bei einem Verantwortlichen beschäftigter Datenschutzbeauftragter nur aus wichtigem Grund abberufen werden kann. Dies auch dann, wenn die Abberufung nicht mit der Erfüllung seiner Aufgaben zusammenhängt, sofern diese Regelung die Verwirklichung der Ziele der DSGVO nicht beeinträchtigt.

De facto eine Nicht-Entscheidung traf der EuGH in einer weiteren Vorlagefrage, diesmal dazu, unter welchen Voraussetzungen das Vorliegen eines „Interessenskonflikts" im Sinne von Art. 38 Abs. 6 DSGVO festgestellt werden kann. Die Bestimmung sei dahin auszulegen, dass ein Interessenskonflikt im Sinne dieser Bestimmung bestehen kann, „wenn einem Datenschutzbeauftragten andere Aufgaben oder Pflichten übertragen werden, die ihn dazu veranlassen würden, die Zwecke und Mittel der Verarbeitung personenbezogener Daten bei dem Verantwortlichen festzulegen." Dies müsse das nationale Gericht im Einzelfall auf Grundlage einer Würdigung aller relevanten Umstände feststellen. Insbesondere sei dabei die Organisationsstruktur des Verantwortlichen im Licht aller anwendbaren – auch internen – Rechtsvorschriften des Verantwortlichen zu berücksichtigen.

4. VKI versus Lauda Motion – Aktivlegitimation unabhängig von der Verletzung konkreter Rechte einer betroffenen Person

Im Verfahren des VKI gegen Laudamotion wegen nicht rechtskonformer Klauseln in den Allgemeinen Beförderungsbedingungen der (ehemaligen) Airline beantragte Laudamotion zunächst Klageabweisung mit dem Argument, dass dem VKI die Klagebefugnis bei Datenschutzklauseln fehlen würde. Das Verfahren war deshalb bis zur Entscheidung des EuGH im Prozess gegen Meta Platforms unterbrochen. Dort bestätigte der EuGH im Frühjahr 2022, dass die DSGVO dem Klagerecht von Verbraucherschutzverbänden wegen Verwendung unzulässiger AGBs nicht entgegensteht. Der EuGH führte damals aus, dass es nicht erforderlich

sei, eine Klagemöglichkeit in Umsetzung der Öffnungsklausel des Art. 80 Abs. 2 DSGVO zu schaffen, wenn es bereits eine nationale Regelung gibt, welche Verbände ermächtigt, entsprechende Unterlassungsklagen zu erheben. Diese liegt in Österreich in der Form des § 29 KSchG vor.

Ausgehend von dieser Entscheidung bestätigte nun auch das OLG Wien im Verfahren gegen die Laudamotion (**2 R 48/20y)** die Aktivlegitimation des VKI. Mit seinem Urteil befand das OLG schließlich die beanstandete (Datenschutz-) Klausel als intransparent, weil den Betroffenen nicht klar gewesen sei, wer die möglichen Empfänger der verarbeiteten Daten seien und zu welchem Zweck sie die Daten bekommen. Die Verarbeitungszwecke seien in den Beförderungsbedingungen nur „allgemein und ausufernd" umschrieben, weshalb die Kund:innen die konkreten Zwecke, zu denen eine Datenverarbeitung erfolgen soll, nicht überschauen konnten.

Eine Verarbeitung personenbezogener Daten ist dann zulässig, wenn sie zur Erfüllung des Vertrages unbedingt erforderlich ist. Die in der Klausel genannten Zwecke – der „Erwerb von Zusatzleistungen wie Hotelbuchungen und Fahrzeuganmietung" oder „Entwicklung und Angebot von Dienstleistungen" – seien aber zur Erfüllung des Beförderungsvertrags nicht notwendig gewesen.

Das Verfahren zeig, dass es bei manchen Unternehmen noch einer besseren Bewusstseinsbildung bedarf, wem welche Daten zu welchen Zwecken weitergeben werden dürfen, so der VKI in einem Kommentar.

5. OGH-Entscheidung zu Kameras im Fitnesscenter: Verweis in AGB nicht ausreichend

Mit einer Entscheidung zur Zulässigkeit von Videoüberwachung im Fitnessstudio (OGH 18.10.2022, 4 Ob 59/22p) bestätigte der OGH vor kurzem die Rechtsmeinung der Arbeiterkammer, dass ein genereller Verweis auf Überwachungskameras in den AGB des Mitgliedsvertrags zur datenschutzkonformen Information der Mitglieder nicht ausreicht. Kundinnen und Kunden müssten vielmehr eigens informiert werden. Konkret hatte die Fitnesskette Cleverfit zur Vermeidung von Straftaten ihre Trainingsräume videoüberwacht und die betroffenen Bereiche mit Schildern ausgewiesen. Dazu formulierte sie in ihren AGB, die Aufnahmen würden „einzelfallbezogen" gespeichert, soweit dies zur „Sicherheit" der Mitglieder und zur „Aufklärung von strafbaren Handlungen sowie zur Abwehr oder Durchsetzung von Schadenersatzansprüchen" erforderlich sei.

Ein klarer Verstoß gegen das Verbot der Koppelung (der datenschutzrechtlichen Einwilligung mit dem generellen Vertragsabschluss), befand der OGH. Die Klausel lasse auch offen, welche konkreten Bereiche überwacht und für welche Sachverhalte und Dauer die Aufzeichnungen gespeichert würden. Eine Klausel in AGB, nach welcher der Vertragspartner der Verwendung seiner personenbezogenen Daten zu Zwecken zustimme, die für die Vertragsabwicklung nicht erforderlich seien, sei daher unzulässig bzw. intransparent.

Fazit: Datenschutzerklärungen in die AGB zu integrieren ist unklug, oft ist ohnehin ein „berechtigtes Interesse" gem. Art. 6 Abs. 1 lit. f DSGVO als Rechtsgrundlage vorhanden.

6. Top 3 DSGVO-Bußgelder im Januar 2023

1. 390 Millionen Euro Bußgeld für Facebook und Instagram

Mit einem rekordverdächtigen Bußgeld i. H. v. knapp 400 Mio. Euro beginnt das (Datenschutz-)Jahr für Meta Platforms Ireland Limited ziemlich teuer. Die Pönale wurde von der irischen Datenschutzbehörde DPC ausgesprochen, die Meta-Töchter Facebook (210 Mio. Euro) und Instagram (180 Mio. Euro) „teilen" sich quasi die Strafe. Meta hatte im Zuge des Inkrafttretens der DSGVO die Rechtsgrundlage für die Verarbeitung personenbezogener Daten in seinen Netzwerken geändert – statt der Einwilligung bezog man sich nunmehr auf Vertragserfüllung nach Art. 6 Abs. 1 Satz 1 lit. b DSGVO. Die Änderung trat für Facebook und Instagram gleichzeitig in Kraft. Die DPC entschied jetzt gegen die Social-Media-Plattform: Das Ausspielen personalisierter Werbung kann nicht auf den Erlaubnistatbestand der Vertragserfüllung gestützt werden und sei somit rechtswidrig.

Fazit: Große Technologieanbieten bleiben am Radar der Aufsichtsbehörden.

2. CNIL bittet TikTok wegen datenschutzwidrigem Cookie-Banner zur Kassa

Die französische Aufsichtsbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) hat zu Jahresbeginn ein Bußgeld von 2 x 2,5 Mio. Euro gegen das chinesische Video-Portal TikTok ausgesprochen. Auch hier teilen sich zwei Gesellschaften die Strafe, die TikTok Information Technologies UK Limited einerseits und die TikTok Technology Limited aus Irland andererseits. Laut CNIL haften beide Gesellschaften als gemeinsame Verantwortliche dafür, auf ihrer Website ein Cookie-Banner benutzt zu haben, bei dem die Ablehnung von Cookies schwieriger war als deren Annahme. Auch die Information der TikTok Besucher*innen über die zu setzenden Cookies wurde von der Behörde als mangelhaft eingestuft.

3. Edison Energia S.p.A

Das im Bereich Elektrizität und Erdgas tätige italienische Energieversorgungsunternehmen Edison S.p.A. hat im Februar 2023 die italienische Datenschutzbehörde mit einer empfindlichen Geldstrafe von ursprünglich knapp 5 Mio. Euro belegt. Das Unternehmen hatte, so die Behörde, wiederholt Personen kontaktiert, ohne dafür eine Zustimmung erhalten zu haben. Auf die Aufforderung, keine unterwünschten Anrufe mehr zu tätigen, reagierte die Edison S.p.A. erst gar nicht. Die Behörde befand des Weiteren die fehlende Möglichkeit für Kund*innen, eine freie und spezifische Einwilligung für verschiedene Zwecke (Werbung, Weitergabe von Daten an Dritte) innerhalb der Website oder App auszudrücken, als nicht datenschutzkonform.

Interessant: Die Edison Energie S.p.A. machte innerhalb der gesetzten Frist von ihrem Recht auf Streitbeilegung Gebrauch und zahlte nur die Hälfte der verhängten Geldbuße.

7. In eigener Sache: Neu an Bord

Mit Menas Saweha wird das Team der Secur-Data mit März 2023 um einen weiteren Berater verstärkt. Nach Tätigkeiten bei den Wiener Linien und der Allianz Insurance war der Jurist zuletzt als Fachreferent bei der Familie und Beruf Management GmbH tätig.

Datenschutz-Seminare 2023

Save the Date: 28. und 29. März 2023: Datenschutz- und IT-Praxisseminare

Auch 2023 bringt eine Reihe von spannenden Neuerungen und Entwicklungen im heimischen und internationalen Datenschutz. Lassen Sie sich im bewährt kleinen Kreis von unseren Top-Expertinnen und -Experten über alle wesentlichen Neuerungen für 2023 in Angelegenheiten der Informationssicherheit und Datenschutzpraxis informieren. Neben praxisnaher Wissensvermittlung steht Secur-Data für State-of-the-Art-Anwendungstipps sowie praxistaugliche Muster und Vorlagen. Auch heuer wieder wird Ihnen **Herr Mag. Andreas Rohner von der österreichischen Datenschutzbehörde** die aktuelle Judikatur der DSB präsentieren und auf Ihre Fragen eingehen.

Hier geht's zur Anmeldung: https://www.secur-data.at oder telefonisch unter (01) 533 42 07-0

Wir freuen uns auf Ihren Anruf!

28. März 2023, 9:15 – 17:00 Uhr: „Rechtsentwicklung und Best Practices"
Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Mag. Sylvia Metenczuk, MAS
Gastreferent: Mag. Andreas Rohner (Datenschutzbehörde Österreich)

29. März 2023, 9:15 – 17:00 Uhr: „Praxis-Updates zu Datensicherheit & Informationssicherheit"
Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Jürgen Stöger

Ort: Hilton Vienna Plaza, Schottenring 11, 1010 Wien

Selbstverständlich stehen wir auch für Inhouse-Schulungen oder Seminare zu Spezialthemen zur Verfügung.

Weitere Informationen und Details finden Sie auf unserer Website https://www.secur-data.at.