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

Dezember 2023 Ausgabe Nr. 109

Liebe Leserinnen und Leser,

Das Jahr 2023 neigt sich langsam dem Ende zu und wir möchten uns für die Zusammenarbeit mit Ihnen bedanken. In dieser Weihnachtsausgabe möchten wir Ihnen spannende Entwicklungen im Datenschutz bescheren: Wegweisende Rechtsprechung der Höchstgerichte, aktuelle Gesetzesvorhaben und die Top-Bußgelder für Datenschutzverstöße.

Ihren Familien und Mitarbeitern wünschen wir erholsame Feiertage und ein gesundes und erfolgreiches neues Jahr 2024!

Mag. Judith Leschanz
Geschäftsführung

1. Schweizer Datenschutzgesetz in Kraft

Am 1. September 2023 trat das vollständig überarbeitete **Schweizer Datenschutzgesetz** (DSG)[1] gemeinsam mit der neuen Datenschutzverordnung (DSV) in Kraft. Dies war ein notwendiger Schritt, denn das ursprüngliche Schweizer Bundesgesetz über den Datenschutz stammt aus dem Jahr 1992.

Mittlerweile sorgen neue Technologien wie Cloud-Dienste, soziale Medien und IoT für regen Datenaustausch zwischen unterschiedlichen Parteien, sodass Änderungen zum adäquaten Schutz der Nutzer notwendig waren. Auch die Kompatibilität des Schweizer Datenschutzes mit der europäischen DSGVO war ein wichtiges Anliegen der Gesetzesrevision, damit die Schweizer Unternehmen EU-weit weiterhin wettbewerbsfähig bleiben.

Ein Überblick über die wichtigsten Neuerungen:

- **Persönlicher Anwendungsbereich**: Nur mehr Daten natürlicher Personen sind betroffen, juristische Personen sind nicht mehr inkludiert (das österreichische DSG umfasst dagegen weiterhin juristische Personen).
- Die Grundsätze **„Privacy by Design“** und **„Privacy by Default”** wurden verankert: Software, Hardware und Dienstleistungen müssen in einer Weise konfiguriert werden, die den Datenschutz gewährleistet und die Privatsphäre der Nutzer respektiert.
- **Folgenabschätzungen** werden verpflichtend, sofern ein hohes Risiko für

[1] https://kurzelinks.de/x9w7

die Persönlichkeits- oder Grundrechte der Betroffenen besteht.

- Der Begriff **Profiling** wurde als „automatisierte Bearbeitung von Personendaten“ zur Bewertung und Vorhersage verschiedener Aspekte natürlicher Personen aufgenommen.
- Das **Verzeichnis der „Bearbeitungstätigkeiten“** wird verpflichtend. Ausgenommen sind KMU, deren Verarbeitung ein geringes Risiko für Betroffene mit sich bringt.

Der Angemessenheitsbeschluss 2000/518/EG[2] der Europäischen Kommission für die Schweiz aus dem Jahr 2000 ist seit Frühjahr 2019 in Revision.

2. EU-Acts-Update

EU-Gremien einigen sich auf AI-Act

Nach einem dreitägigen Verhandlungsmarathon haben sich die Verhandler des Europäischen Rates und des Europäischen Parlaments auf einen gemeinsamen Text zur weltweit ersten KI-Regulierung, dem AI-Act, geeinigt[3]. Ziel des Verordnungsentwurfs, der auf einen Vorschlag der Kommission aus dem Jahr 2021 zurückgeht, ist es, den grundrechtskonformen und ethisch verantwortlichen Einsatz von KI-Systemen im europäischen Markt zu ermöglichen. Zwar hat US-Präsident Joe Biden per Exekutivverordnung[4] eine KI-Regulierung in den Vereinigten Staaten angeordnet und auch in China sind seit August KI-Gesetze[5] in Kraft, jedoch ist der europäische AI-Act in seinem Umfang und Anwendungsbereich deutlich fortgeschrittener und detaillierter.

Der Text wurde jedoch noch nicht konsolidiert. Dies könnte mehrere Wochen in Anspruch nehmen, da zwar eine vorläufige politische Einigung erzielt wurde, viele Details aber noch ausgearbeitet werden müssen. Immerhin sollen Fehler vermieden werden, die nationales Gold-Plating oder die unpräzise Umsetzung des Gesetzes ermöglichen, wie dies bei der DSGVO passiert ist und derzeit eine Revision notwendig macht. Der AI-Act soll in etwa zwei Jahren in Kraft treten, wobei bestimmte Teile der Verordnung bereits zuvor wirksam werden sollen.

Unter anderem wurde der sachliche Anwendungsbereich im Trilog kontrovers debattiert. Dabei geht es darum, welche Technologien der künstlichen Intelligenz unter den AI-Act fallen und reguliert werden sollen. Der risikobasierte Ansatz sieht vor, dass KI-Systeme mit höherem Schadensrisiko umfangreicheren Auflagen unterworfen werden. Das EU-Parlament hat sich gegen den Widerstand vor allem Deutschlands und Frankreichs in puncto Transparenz- und Offenlegungspflichten von KI-Basismodellen (Foundation Models, zB GPT-4) durchgesetzt und umfangreiche Bestimmungen festgelegt, die für kleinere Start-ups bestimmt eine ressourcentechnische Herausforderung darstellen werden.

Wie die DSGVO und andere digitale Rechtsakte der EU sieht auch der AI-Act beträchtliche Geldbußen für Verstöße vor. Für den Fall, dass ein Unternehmen verbotene KI-Systeme auf dem Markt einführt, steht eine Geldstrafe von sieben Prozent des Jahresumsatzes oder 35 Mio. EUR im Raum, zur Anwendung kommt die höhere der beiden Summen. Für sonstige Verstöße kommen Strafen in Höhe von drei Prozent des Jahresumsatzes oder 15 Mio. EUR zur Anwendung. Wenn ein Unternehmen falsche Informationen über die KI erteilt, wird

[2] https://kurzelinks.de/4yip

[3] https://kurzelinks.de/vxqp

[4] https://kurzelinks.de/6ho3

[5] https://kurzelinks.de/w4ed

eine Geldbuße von 1,5 Prozent des Jahresumsatzes oder 7,5 Mio. EUR verhängt.

Der Data Act wurde verabschiedet

Am 27. November 2023 erteilte der Rat der Europäischen Union die endgültige Genehmigung des Datengesetzes (Data Act)[6] und schloss damit das Gesetzgebungsverfahren ab. Der am 23. Februar 2022 von der EU-Kommission eingebrachte Vorschlag konzentriert sich auf die Regelung des fairen Zugangs und der fairen Nutzung von Daten.

Insbesondere regelt es die Weitergabe von Daten an Verbraucher (B2C) und zwischen Unternehmen (B2B) sowie deren Bereitstellung für öffentliche Stellen bei außergewöhnlicher Notwendigkeit (B2G). Darüber hinaus beinhaltet das Datengesetz sowohl ein Verbot von missbräuchlichen Vertragsklauseln für KMU als auch vertragliche und technische Regelungen für den Wechsel zwischen Datenverarbeitungsdiensten („Cloud-Switching“).

Beim Datengesetz handelt es sich um eine Verordnung, die unmittelbar in der gesamten EU gilt, mit einer Übergangsfrist von 20 Monaten nach der Veröffentlichung im EU-Amtsblatt. Eine Ausnahme bildet jedoch Art. 3 Abs. 1 DA, der erst 32 Monate nach Inkrafttreten der Verordnung gilt und für Produkte, die ab diesem Zeitpunkt auf den Markt kommen, standardmäßig einen einfachen, sicheren und kostenlosen Zugang zu Nutzerdaten vorschreibt.

Als Teil der europäischen Datenstrategie neben AI-Act und Digital Markets Act zielt der Data Act darauf ab, die EU als Vorreiterin einer datengesteuerten Wirtschaft zu etablieren und den gleichberechtigten Zugang zu Daten sicherzustellen. Erklärtes Ziel ist es, allen Beteiligten der Datenwirtschaft gleichberechtigten Zugang zu Industriedaten zu ermöglichen und ungenutztes Potenzial freizusetzen, indem die Nutzbarkeit industrieller Daten verbessert wird. Darüber hinaus wird versucht, den Markteinfluss von großen Unternehmen und Plattformen („Gatekeepern“) auf KMU und Verbraucher umzuverteilen und einen Binnenmarkt für Daten zu entwickeln.

3. Privacy by Design: neue Norm ISO 31700

Eine der Anforderungen der Datenschutz-Grundverordnung (DSGVO) betrifft die Notwendigkeit, Datenschutz durch Technikgestaltung – auch als „Privacy by Design“ bezeichnet – gemäß **Artikel 25 DSGVO**[7] zu gewährleisten.

Ziel dieses datenschutzrechtlichen Grundsatzes ist es, Datensicherheit bereits im Entwicklungsprozess von Produkten bzw. Systemen zu bedenken und integrieren. Dadurch sollen Datenschutzrisiken minimiert und die Einhaltung der gesetzlichen Bestimmungen sichergestellt werden, ohne die Betroffenen unnötig zu belasten. Diese Anforderungen finden sich in der ISO-Norm 31700 wieder und behandeln einerseits Verfahren zur Produktgestaltung, das User-Interface, die Verbraucherkommunikation, Tests und Maßnahmen für Einstellungen etc. (ISO 31700-1)[8], anderseits Beispiele zum Standard-Einsatz (ISO 31700-2).[9]

Durch die Umsetzung der globalen Norm zur Standardisierung von Privacy by Design wird das Vertrauen der Verbraucher zu ihren Diensteanbietern gestärkt. Unternehmen, die regelmäßig mit der Entwicklung von Systemen und Dienstleistungen befasst sind, sollten die Umsetzung dieser Norm bzw. zumindest die Orientierung an den enthaltenen Anforderungen unbedingt in Betracht ziehen.

[6] https://kurzelinks.de/cu48

[7] https://www.dsgvo-portal.de/dsgvo_artikel_25.php

[8] https://www.iso.org/standard/84977.html

[9] https://www.iso.org/standard/84978.html

SecurWhistle®

Das **HinweisgeberInnenschutzgesetz (HSchG)** verpflichtet Unternehmen und öffentliche Einrichtungen ab 50 Beschäftigten, bis **17. Dezember 2023** ein Hinweisgebersystem einzurichten. Bei über 250 Mitarbeitenden trat die Pflicht bereits am 25. August 2023 in Kraft.

Das Gesetz sieht die Möglichkeit vor, externe Hinweisprüfer zu beauftragen. Mit **SecurWhistle®** implementieren Sie einen sicheren digitalen Meldekanal und erhalten eine individuelle und professionelle Verwaltung der einlangenden Meldungen durch unsere Berater.

Ihre Vorteile:

- ✅ Absolute Anonymität: Unser Whistleblowing-Tool schützt die Identität des Hinweisgebers zu 100 %. Die verschlüsselte Plattform gewährleistet, dass keinerlei Informationen zurückverfolgt werden können.
- ✅ Wir schulen Ihre Führungskräfte und Betriebsräte in die gesetzlichen Vorgaben des HinweisgeberInnenschutzgesetzes (HSchG) ein und beraten Sie bei der Implementierung eines effizienten Meldeprozesses. Außerdem erhalten Sie von uns ein Infoblatt zum Hinweisgebersystem für Ihre MitarbeiterInnen.
- ✅ Bei Hinweisen mit dringendem Handlungsbedarf erhalten Sie von uns außerdem Handlungsempfehlungen, wie mit dem Fall umzugehen ist.
- ✅ DSGVO-konforme Implementierung des Hinweisgebersystems durch unsere bereitgestellten Unterlagen (Verarbeitungsverzeichnis, Datenschutzinformation, Richtlinien)

Auf Anfrage:

- ✅ Sie erhalten bei Bedarf eine auf Ihr Unternehmen abgestimmte Betriebsvereinbarung gemäß § 96 Abs. 1 Z 3 ArbVG (Kontrollmaßnahmen, welche die Menschenwürde berühren).

Kontaktieren Sie uns für ein kostenloses Erstgespräch und Preisanfragen!

4. Neues aus der Rechtsprechung

Judikatur zum § 165 Abs. 3 TKG 2021

Die Interessenvertretung von Tageszeitungen, Wochenzeitungen und Magazinen hatte bei der österreichischen Datenschutzbehörde einen Antrag auf Genehmigung von Verhaltenskodizes für Presse- und Zeitschriftenmedienunternehmen gemäß Art. 40 Abs. 5 DS-GVO gestellt. Die DSB stimmte dem Verhaltenskodex teilweise zu, lehnte jedoch einige Punkte ab, darunter insbesondere Punkt D.1.3 zur Verarbeitung „notwendiger" Cookies. Dabei geht es um die Verarbeitung personenbezogener Daten ohne Einwilligung zu bestimmten Cookies, weil diese für die Erbringung von Dienstleistungen „erforderlich" im Sinne des Art. 6 Abs. 1 lit. f DSGVO seien.

In der Entscheidung vom 31. Oktober 2023[10] wies der VwGH die Berufung gegen den DSB-Bescheid zurück: Die Richtlinie 2002/58/EG bzw. die entsprechende TKG-Bestimmung

[10] https://kurzelinks.de/w2jo

sehen das berechtigte Interesse als Rechtsgrundlage der Verarbeitung nicht vor. Das „wirtschaftliche Interesse" der Website-Betreiber kann nicht als Basis für das Setzen von Cookies ohne Einwilligung der Nutzer herangezogen werden.

Diese Auslegung zeigt, dass was gem. Richtlinie 2002/58/EG als „unbedingt erforderlich" gilt, nicht auf die gleiche Weise betrachtet werden kann wie die Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO. Jedenfalls darf der Begriff „unbedingt erforderlich" in § 96 Abs. 3 TKG 2003 (nunmehr § 165 Abs. 3 TKG 2021) nicht so ausgelegt werden, dass auch ein wirtschaftliches Interesse die Notwendigkeit des Einsatzes von Cookies begründet. In diesem Sinne zulässig sind ausschließlich Cookies, die für die Übertragung oder zur Bereitstellung eines vom Nutzer geforderten Dienstes notwendig sind. Für alle weiteren muss die Einwilligung durch den Nutzer erteilt werden.

EuGH-Urteil zur Verhängung von Geldbußen (Deutsches Wohnen)

Der Europäische Gerichtshof (EuGH) hat kürzlich in einem Urteil (Rechtssache C-807/21)[11] entschieden, dass Geldbußen gegen juristische Personen wie Unternehmen grundsätzlich zulässig sind. Im spezifischen Fall der „Deutsche Wohnen SE" könnte das zuvor aufgehobene Bußgeld von über 14 Mio. EUR wieder wirksam werden.

Der Deutsche Wohnen SE wurde vorgeworfen, dass sie personenbezogene Daten von Mietern ihrer Tochterunternehmen unrechtmäßig lange gespeichert hat. Diese Daten, einschließlich sensibler Informationen wie Identitätsnachweise, Steuer-, Sozial- und Krankenversicherungsdaten, waren auch nach dem Auszug der Mieter noch einsehbar, obwohl die Aufbewahrungsfristen abgelaufen waren. Nach einem ersten Hinweis der Aufsichtsbehörde im Jahr 2017 wurde 2019 ein Bußgeld verhängt, da die Deutsche Wohnen SE es vorsätzlich versäumte, diese Daten zu löschen.

Nach deutschem Recht (§ 30 OWiG) wurde aber argumentiert, dass eine Ordnungswürdigkeit nur von einer natürlichen Person begangen und dieser zugerechnet werden kann, nicht jedoch einer juristischen Person. Der Fall gelangte vor das Kammergericht Berlin, das dem EuGH folgende Fragen vorgelegt hat:

1. Kann ein Bußgeldverfahren gegen ein Unternehmen durchgeführt werden, ohne dass ein Fehlverhalten einer identifizierten natürlichen Person festgestellt wird?
2. Muss das Unternehmen den durch einen Mitarbeiter vermittelten Verstoß schuldhaft begangen haben oder reicht ein objektiver Verstoß gegen die DSGVO aus, um das Unternehmen zu bestrafen („strict liability")?

Der EuGH stellte fest, dass laut Art. 83 Abs. 3 iVm Art. 4 Z 7 DSGVO auch juristische Personen für Datenschutzverstöße verantwortlich sein können. Es sei nicht zwingend erforderlich, die natürliche Person zu identifizieren, die den Verstoß begangen hat. Jedoch betonte der EuGH, dass Vorsatz oder Fahrlässigkeit eine Rolle spielen müssen, um Geldbußen gemäß der DSGVO zu verhängen.

Es bleibt abzuwarten, wie das Berliner Kammergericht den Nachweis von Vorsatz und Fahrlässigkeit im Fall der Deutschen Wohnen bewerten wird. Das Urteil hat potenziell weitreichende Auswirkungen auf die Handhabung von Bußgeldverfahren gegen Unternehmen und die Bewertung von Vorsatz und Fahrlässigkeit bei juristischen Personen nach geltendem Recht.

Kein immaterieller Schadenersatz bei verspäteten Auskünften nach Art. 15 DSGVO

Das ArbG Duisburg verurteilte zunächst ein Immobilienunternehmen zu einer Zahlung von EUR 10.000 an ehemalige Mitarbeiter wegen verspäteter Auskunftserteilung. Das Unter-

[11] https://kurzelinks.de/csnq

nehmen legte dagegen Berufung vor dem LAG Düsseldorf ein, das diese Entscheidung vollständig aufhob.[12]

Auch wenn aufgrund der Nichterfüllung des Anspruchs ein Verstoß gegen das Recht auf Auskunft nach DSGVO vorliegt, entschied das LAG Düsseldorf, dass dies nicht automatisch zu einem Schadenersatzanspruch nach Art. 82 DSGVO führt. Art. 82 DSGVO (iZm ErwGr 146) setzt für die Haftungsbegründung einen Verstoß gegen die DSGVO-bezogene Datenverarbeitung voraus. Die Nichteinhaltung der Auskunftspflicht nach Art. 15 DSGVO, sei es verspätet oder unvollständig, erfüllt diese Voraussetzung nicht. Darüber hinaus verlangt Art. 82 mehr als nur einen bloßen Verstoß gegen die Bestimmungen der DSGVO, um eine Entschädigung für immateriellen Schäden zu fordern. Der Anspruch des Klägers auf Kontrollverlust über die Daten reicht nicht aus und kommt im Wesentlichen einem Verstoß gegen Art. 15 DSGVO gleich. Darüber hinaus machte der Kläger keine konkreten Angaben zu etwaigen zusätzlichen emotionalen Schäden.

5. Top 3 DSGVO-Bußgelder

Millionenbußgeld in Norwegen aufgrund von Datenschutzverletzungen

Die norwegische Aufsichtsbehörde, Datatilsynet, hat der Arbeits- und Wohlfahrtsverwaltung (NAV) ein Bußgeld von ca. EUR 1.706.994 auferlegt. In ihrer Überprüfung stellte die Behörde fest, dass die NAV, die den Bürgern des Landes verschiedene Leistungen wie Rente, Kindergeld und Sozialhilfe bereitstellt, personenbezogene Daten nicht DSGVO-konform verarbeitet hat. Mitarbeiter hatten zu weitreichenden Zugang zu sensiblen Daten und NAV protokollierte nicht, in welchem Umfang auf die IT-Systeme zugegriffen wird. Zudem versäumte es die Verwaltung, angemessene Schulungen für Administratoren bereitzustellen. Die festgestellten Mängel sowie die Verarbeitung besonderer Kategorien personenbezogener Daten führten zur Verhängung des hohen Bußgeldes gemäß den Bestimmungen der DSGVO.

Kein Spielraum für DSGVO-Verletzungen unter dem Deckmantel „Nice-to-have“

Die spanische Aufsichtsbehörde (AEPD) hat aufgrund der Beschwerde einer betroffenen Person ein Bußgeld in Höhe von EUR 72.000 gegen das Eurocollege Oxford English Institute wegen übermäßiger Datensammlung verhängt. Die Schule verlangte von zukünftigen Flugbegleitern Gesundheitsprüfungen, Gesundheitszeugnisse, eine Erklärung zum Gesundheitszustand und Führungszeugnisse als Bedingung für die Einschreibung. Die AEPD stellte jedoch fest, dass diese Datenerhebung weder erforderlich noch gesetzlich vorgeschrieben war.

Das Bußgeld erinnert wieder an die Wichtigkeit des Prinzips der Datenminimierung. Es ist entscheidend, Daten ausschließlich im absolut notwendigen Umfang zu sammeln. Die Verarbeitung von Gesundheitsdaten und Führungszeugnissen ohne klaren Zweck widerspricht grundlegenden Datenschutzprinzipien.

Gesundheitsdaten in verlassenem Krankenhaus gefunden

Ein anonymer Hinweis an die italienische Aufsichtsbehörde (GPDP) enthüllte, dass in einem verlassenen Sanatorium sensible Gesundheitsdaten ungeschützt zugänglich waren. Patientenakten mit hochsensiblen Informationen, einschließlich Röntgenbildern, lagen frei herum. Die Gesundheitsbehörde der Toskana hatte offensichtlich ihre Pflicht vernachlässigt, diese Daten zu vernichten oder sicher zu

[12] https://kurzelinks.de/1geo

verwahren. Als Konsequenz wurde ein Bußgeld in Höhe von EUR 50.000 verhängt.

Diese Ereignisse unterstreichen die Notwendigkeit von Maßnahmen, um sicherzustellen, dass sensible Informationen auch dann vor unbefugtem Zugriff geschützt bleiben, wenn sie nicht mehr benötigt werden. Insbesondere bei Patientenakten ist der verantwortungsbewusste Umgang essenziell, um die Integrität und Vertraulichkeit der Gesundheitsdaten zu gewährleisten.

••••