

DSG-Info-Service

Jänner 2024

Ausgabe Nr. 110

Liebe Leserinnen und Leser,

herzlich willkommen im neuen Jahr und zu einer neuen Ausgabe unserer DSG-Info! In dieser Ausgabe werfen wir einen kritischen Blick auf die Entwicklung der Datenschutz-Grundverordnung (DSGVO) seit ihrer Einführung und den neuen Bericht des Europäischen Datenschutzausschusses über die Rolle des Datenschutzbeauftragten. Außerdem präsentieren wir Ihnen spannende Erkenntnisse aus der datenschutzrechtlichen Rechtsprechung. Wie immer erhalten Sie einen Überblick über die wichtigsten Bußgelder des vergangenen Monats und relevante Ankündigungen!

Viel Spaß bei der Lektüre wünscht

*Mag. Judith Leschanz
Geschäftsführung*

1. Newsmeldungen

5 Jahre DSGVO – Die Evaluierung

Die Datenschutz-Grundverordnung (DSGVO) ist seit ihrer Geltung im Mai 2018 das zentrale Element des europäischen Datenschutzrechts. Anlässlich ihrer zweiten Evaluierung 2024 werden zahlreiche Diskussionen zur Effektivität und den Auswirkungen dieser Verordnung geführt. Einige dieser Punkte möchten wir für Sie hier festhalten.

Die Rolle des **Datenschutzbeauftragten** hat sich als unerlässlich für Unternehmen erwiesen. Die damit verbundene Querschnittskompetenz wird vor allem von **KMU** geschätzt, da er in vielen Bereichen teure Fachberater ersetzen kann. Er berät den Verantwortlichen bei der gesetzeskonformen Planung und Durchführung im gesamten Lebenszyklus der Verarbeitung personenbezogener Daten und prüft die

Effektivität der getroffenen Schutzmaßnahmen, beispielsweise durch interne Audits.

Die DSGVO schreibt Verantwortlichen, insbesondere in den **Art. 5, 24 und 32 DSGVO**, beträchtliche Pflichten vor, die sie bei der Verarbeitung personenbezogener Daten einzuhalten haben. Diese Pflichten beinhalten präventive **technische und organisatorische Maßnahmen** (TOM) sowie die stetige Prüfung und Aktualisierung dieser Maßnahmen. Überschießende Bürokratie und risikounabhängige Auflagen erschweren die Wahrnehmung dieser Aufgaben. Hinzu kommt, dass die **Entwickler** digitaler Lösungen von der DSGVO weitgehend unberührt bleiben, was zu einer (oft nicht verhältnismäßigen) Verlagerung der Belastungen zum Verantwortlichen führt.

Die mit der Umsetzung der DSGVO verbundene Bürokratie schlägt sich in verschiedenen

Dokumentations-, Organisations- und Hinweispflichten nieder. Sie erhöhen Aufwand und Kosten, da auch typische, weit verbreitete Verarbeitungen personenbezogener Daten eine Kette an Pflichten auslösen.

Nehmen wir als Beispiel die Verarbeitung von Personalstammdaten in einem Unternehmen: Für eine rechtmäßige Verarbeitung ist zunächst eine Rechtsgrundlage nach **Art. 6 DSGVO** zu wählen. Diese Verpflichtung wird durch die Dokumentation nach **Art. 5 Abs. 2 DSGVO** (Rechenschaftspflicht), die Informationspflichten nach **Art. 13-14 DSGVO** und die Erfassung der Verarbeitung im Verzeichnis der Verarbeitungstätigkeiten nach **Art. 30 DSGVO** erweitert. Jede dieser Verpflichtungen unterliegt eigenen Modalitäten, da jedes Mal Zweck und Adressat wechseln.

Diese Anforderungen stellen für Unternehmen oft eine erhebliche finanzielle Belastung dar. Besonders für KMU erscheinen die Herausforderungen aus der DSGVO oft überwältigend. Sie verfügen im Allgemeinen nicht über die Ressourcen und das notwendige Fachwissen, um den komplexen Vorgaben gerecht zu werden. Dies kann auch zu einem Wettbewerbsnachteil gegenüber größeren Unternehmen führen. Es wäre daher wünschenswert, dass zukünftige Anpassungen eine differenziertere Betrachtung der Unternehmensgröße und angemessene Erleichterungen für KMU vorsehen.

Ein weiterer bedeutender Aspekt in Zeiten der zunehmenden Digitalisierung ist die **Haftung der Hersteller** digitaler Anwendungen und Lösungen. Die DSGVO legt fest, dass sowohl Verantwortliche als auch Auftragsverarbeiter zur Einhaltung der Verordnung verpflichtet sind. Datenschutzrechtliche Probleme dort zu lösen, wo sie häufig entstehen, nämlich beim Hersteller, hat der EU-Gesetzgeber bei der Formulierung des Art. 25 DSGVO verabsäumt.

Die Problematik zeigt sich deutlich anhand von **Art. 25 Abs. 2 DSGVO**: Verantwortliche stehen vor der praktischen Herausforderung, angemessene technische und organisatorische Maßnahmen zu implementieren, oft fehlt es aber an geeigneter Hard- bzw. Software. Diese wird von externen Herstellern bereitgestellt, die nur bestimmte Konfigurationsmöglichkeiten zur Verfügung stellen. In Bezug auf diese Konfigurationen gilt selbstverständlich die Verpflichtung aus Art. 25 Abs. 2 DSGVO, datenschutzfreundliche Optionen zu wählen. Insgesamt führt dies dennoch zum mangelhaften Schutz personenbezogener Daten, da der Verantwortliche, auch aufgrund seiner benachteiligten Verhandlungsposition gegenüber dem Hersteller, nur über begrenzte Einflussmöglichkeiten verfügt.

Zusammenfassend lässt sich sagen, dass die DSGVO seit ihrem Inkrafttreten überwiegend positive Veränderungen bewirkt hat. Dennoch verbleiben Herausforderungen, insbesondere im Hinblick auf die damit verbundene Bürokratie und die oft unverhältnismäßige Belastung der KMU. Die kontinuierliche Überprüfung und Anpassung der Verordnung, klare Leitlinien und Haftungsverpflichtungen für Entwickler könnten dazu beitragen, die DSGVO effizienter und praxistauglicher zu gestalten.

EDSA-Bericht zur Rolle des Datenschutzbeauftragten

Im Laufe des vergangenen Jahres haben sich 25 Datenschutzbehörden im gesamten Europäischen Wirtschaftsraum (EWR) an einer Untersuchung zum Thema Benennung und Position des Datenschutzbeauftragten beteiligt. Mehr als 17.000 Antworten von verschiedenen Organisationen und Datenschutzbeauftragten sowohl aus dem öffentlichen als auch dem privaten Sektor wurden analysiert. Der [Bericht¹](#) verleiht einen interessanten Einblick in Arbeit

¹ <https://kurzelinks.de/xn6o>

und Position von Datenschutzbeauftragten fünf Jahre nach Geltung der DSGVO.

Die geäußerten Bedenken und Herausforderungen betreffen unter anderem unzureichende Ressourcen oder Fachkenntnisse der Datenschutzbeauftragten, mangelnde Unabhängigkeit, fehlende Berichtsmöglichkeiten an die Unternehmensführung oder gar das Unterlassen der Bestellung eines Datenschutzbeauftragten trotz gesetzlicher Verpflichtung. Dabei variieren die Ausprägung und Intensität dieser

Herausforderungen zwischen den Mitgliedstaaten der EU. Ebenfalls einen Unterschied macht es, ob der Datenschutzbeauftragte im privaten oder öffentlichen Sektor, wo vor allem die Freigabe finanzieller Ressourcen komplexer sein kann, tätig ist.

Zusätzlich enthält der Bericht Empfehlungen, die Organisationen und Datenschutzbeauftragten bei der Bewältigung der festgestellten Herausforderungen unterstützen können.

2. Neues aus der Rechtsprechung

Fristlose Kündigung im Mietrecht: Verwertung der Videoaufnahme trotz fehlender Einwilligung

Das Landgericht Essen fällt kürzlich ein interessantes Urteil² in einem Mietrechtsstreit, das nicht nur aufgrund der schweren Verstöße der Mieter, sondern auch wegen der Zulassung von Videoaufnahmen als Beweismittel für Aufsehen sorgte. Die Mieterin hatte ihre Vermieterin beleidigt und bedroht, was schließlich zur fristlosen Kündigung des Mietverhältnisses führte.

Besonders bemerkenswert an dieser Entscheidung war die Zulassung von Videoaufnahmen, für die keine Einwilligung vorlag, als Beweismittel. Die Klägerin legte ein Video vor, das die Beleidigungen und Drohungen der Beklagten zeigte. Obwohl die Beklagte der Aufnahme nicht zustimmte, wurde zwischen den Parteien diskutiert, ob die Aufnahme tatsächlich heimlich gemacht wurde. Das Video wurde aus dem Innenhof aufgenommen und zeigte das Fenster, in dem die Beklagte stand, sie wurde frontal gefilmt. Trotz der geäußerten Bedenken der Beklagten bezüglich einer möglichen Verletzung ihres Persönlichkeitsrechts entschied das Gericht, dass die Aufnahme verwendet werden kann. Es wurde argumentiert, dass die Beklagte

aufgrund ihrer Lautstärke damit rechnen musste, dass auch andere Personen ihre Äußerungen hören können, und dass ihre Aussagen daher öffentlich waren. Darüber hinaus zieht laut Gericht die rechtswidrige Beschaffung allein nicht automatisch ein Beweisverwertungsverbot nach sich.

Das Gericht wog das öffentliche Interesse an Wahrheitsfindung und Rechtspflege gegen das Persönlichkeitsrecht der Beklagten ab. Schließlich befand es, dass das Interesse der Kläger an der Beweiserhebung die Persönlichkeitsverletzung der Beklagten überwog.

EuGH-Entscheidung: Verarbeitung von Gesundheitsdaten unter strengen Auflagen

Der Europäische Gerichtshof (EuGH) hat in einem Urteil vom 21. Dezember 2023 ([Rs. C-667/21](#))³ die Bedingungen für die Zulässigkeit der Verarbeitung von Gesundheitsdaten und damit verbundene Schadenersatzansprüche beleuchtet. Das Vorabentscheidungsersuchen betraf die Verarbeitung von Gesundheitsdaten eines Arbeitnehmers durch einen medizinischen Dienst, der gleichzeitig Arbeitgeber des Betroffenen ist. Die Auslegung und Anwendung von Art. 9, Art. 6 und Art. 82 standen dabei im

² LG Essen – Az.: 10 S 122/23 – Beschluss vom 06.11.2023

³ <https://kurzelinks.de/zpzh>

Vordergrund, d.h. welche Bedingungen für die rechtmäßige Verarbeitung von Gesundheitsdaten zu beachten sind und welchen Zwecken der Schadenersatz dient.

Der EuGH stellte klar, dass jede Datenverarbeitung nicht nur den spezifischen Anforderungen des Art. 9 entsprechen, sondern immer auch die allgemeinen Voraussetzungen des Art. 6 Abs. 1 DSGVO erfüllen muss.

Weiters hob das Gericht hervor, dass der Schadenersatz gemäß Art. 82 DSGVO ausschließlich den Zweck verfolgt, den erlittenen Schaden für die betroffene Person vollständig auszugleichen. Abschreckung oder Bestrafung sind dagegen keine Funktionen des Schadenersatzes, er hat nur eine Ausgleichsfunktion. Daher hat die Schwere eines Verstoßes keinen Einfluss auf die Bemessung der Schadenersatzhöhe.

Ein weiterer relevanter Aspekt betraf die Voraussetzungen für die Haftung: Hierbei wurde die Beweislastumkehr hervorgehoben; beim Verantwortlichen muss jedenfalls Verschulden

vorliegen. Aufgrund der Ausgleichsfunktion des Schadenersatzes hat der Grad des Verschuldens jedoch keinen Einfluss auf die Höhe des Schadenersatzes.

Entscheidungen aus österreichischer Sicht

Nach dem wegweisenden Erkenntnis des EuGH vom 5. Dezember 2023 (C 807/21, wir berichteten in unserer [DSG-Info Nr. 109⁴](#)), wonach juristische Personen unmittelbar bestraft werden können, nimmt die österreichische Datenschutzbehörde alle Strafverfahren wieder auf, die sie gem. § 38 AVG ausgesetzt hatte.

Weiters erkannte der EuGH (C 33/22)⁵ am 16. Jänner 2023 die Zuständigkeit der Datenschutzbehörde für parlamentarische Untersuchungsausschüsse an und stellte fest, dass sich auch diese an die Datenschutzgrundverordnung halten müssen.

Die DSB (2023-0.594.826 vom 18. Dezember 2023) sieht sich nicht zuständig für Rechtsfragen von internationalen Organisationen, welche auf österr. Gebiet angesiedelt sind.

3. Top 3 Bußgelder

Gemeinde bestellt keinen Datenschutzbeauftragten

Die Gemeinde Kourou im französischen Übersee-Département Französisch-Guayana fasste gleich zwei [Geldbußen⁶](#) von der Commission Nationale de l'Informatique et des Libertés (CNIL, franz. Datenschutzbehörde) aus. Schon 2022 bemängelte die Aufsichtsbehörde das Fehlen eines Datenschutzbeauftragten für die Gemeindeverwaltung. Als die Übersee-Gemeinde der Aufforderung, einen Datenschutzbeauftragten zu bestellen, nicht nachkam und somit die **Art. 31 und 37 ff. DSGVO** verletzte,

wurde gegen sie Anfang 2023 eine Geldstrafe in der Höhe von **EUR 5.000** ausgesprochen. Aus unerfindlichen Gründen ließ Kourou die neuerlich gesetzte Frist zur Bestellung des Datenschutzbeauftragten wieder verstreichen, weshalb die Datenschutzbehörde erneut eine **EUR 5.000**-Strafzahlung anordnete. Darüber hinaus muss Kourou für jeden Tag, an dem sie den Anforderungen der CNIL nicht nachkommt, die zusätzliche Strafzahlung von EUR 150 entrichten.

⁴ <https://kurzelinks.de/c34a>

⁵ <https://kurzelinks.de/k3k3>

⁶ <https://kurzelinks.de/19md>

KFZ-Kennzeichen rechtswidrig veröffentlicht

Ein Betroffener legte bei der griechischen Datenschutzbehörde Beschwerde gegen ein Leasingunternehmen ein. Beschwerdegrund waren Immobilienanzeigen des Unternehmens, auf denen KFZ-Kennzeichen erkennbar abgebildet waren. Der Betroffene, dessen KFZ-Kennzeichen auf einer der Anzeigen zu sehen war, hatte mit finanziellen Schwierigkeiten zu kämpfen und sah sich daher gezwungen, seine Immobilie zu verkaufen. Als ein Bekannter von ihm die Anzeigen empfing, erkannte er sofort das Kennzeichen des Betroffenen und erhielt dadurch Aufschluss über seine finanziellen Umstände. Auf Nachfragen und ein Ersuchen des Beschwerdeführers auf Löschung wurde nicht reagiert, weswegen gegen das Leasingunternehmen ein [Bußgeld](#)⁷ in der Höhe von **EUR 20.000** für die Verletzung der **Art. 5 Abs. 1 lit. c DSGVO** und **Art. 15 DSGVO** verhängt wurde.

Britisches Militär veröffentlicht Daten von Ortskräften

An diesem Vorfall zeigt sich, wie bedrohlich Unachtsamkeit des Verantwortlichen werden

kann: Im September 2021 hatte die für Umsiedlungen zuständige Abteilung des britischen Militärs eine E-Mail an 265 afghanische Staatsangehörige verschickt, die für eine Ausreise in Frage kamen. Da die Empfängeradressen in das CC-Feld eingetragen wurden, statt die BCC-Funktion zu verwenden, war die Identität der Empfänger für den gesamten Adressatenkreis sichtbar. Bei einigen Adressen war sogar ein Porträt des Inhabers gespeichert. Diese versehentliche Weitergabe von Informationen war für die betroffenen Helfer extrem gefährlich, insbesondere im Fall des Zugriffs feindlicher Parteien wie der Taliban auf die E-Mail.

Ursprünglich hatte das Information Commissioner's Office aufgrund der Verletzung von **Art. 25 UK GDPR** eine [Strafzahlung](#)⁸ von 1 Mio. Pfund vorgesehen. Aufgrund der täglichen Herausforderungen, mit denen die betreffende Abteilung konfrontiert ist, wurde diese aus Kulanz auf **350.000 Pfund** (ca. EUR 410.000) reduziert.

4. Data Privacy Day

Der kommende Sonntag, der 28. Jänner, markiert den jährlichen Datenschutztag, auch als **Data Privacy Day** bekannt. Dieser Tag wurde ins Leben gerufen, um das Bewusstsein für die Bedeutung der Privatsphäre und den Schutz personenbezogener Daten zu stärken. In einer zunehmend digitalisierten Welt, in der persönliche Informationen oft online gestellt werden,

gewinnt der Datenschutz zunehmend an Relevanz.

Der Privacy Day soll die Menschen erinnern, die Datenschutzeinstellungen ihrer Online-Profile zu überprüfen, starke Passwörter zu verwenden und sich bewusst zu sein, welche Informationen sie mit anderen teilen.

⁷ <https://kurzelinks.de/vzil>

⁸ <https://kurzelinks.de/5x2q>

5. Österreichische Datenschutzbehörde unter neuer Leitung

Die Bundesregierung hat Bundespräsidenten Alexander Van der Bellen den bisherigen Stellvertreter **Dr. Matthias Schmidl** als Leiter der österreichischen Datenschutzbehörde vorgeschlagen. Er folgt damit der seit November pensionierten bisherigen Leitung Dr. Andrea

Jelinek nach. Als seine Stellvertretung wurde MMag. Elisabeth Wagner vorgeschlagen.

Wir gratulieren herzlichst und wünschen gutes Gelingen für die neuen Aufgaben und Herausforderungen!

•••

Datenschutz-Seminare 2024

Die Entwicklung des nationalen und internationalen Datenschutzes geht weiter, auch 2024 sind neue rechtliche Entscheidungen und Aktualisierungen zu erwarten. Lassen Sie sich im bewährten kleinen Kreis von unseren Top-Expertinnen und -Experten über alle wesentlichen Neuerungen 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 wird Ihnen wieder **Herr Mag. Andreas Rohner von der österreichischen Datenschutzbehörde** die aktuelle Judikatur der DSB präsentieren und auf Ihre Fragen eingehen.

8. April 2024, 9:15 – 17:00 Uhr:

„Rechtsentwicklung und Best Practices“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Menas Saweha, Rona Paca

Gastreferent: Mag. Andreas Rohner (Datenschutzbehörde Österreich)

9. April 2024, 9:15 – 17:00 Uhr:

„Praxis-Updates zu Datensicherheit & Informationssicherheit“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Krzysztof Müller, Friedrich Tuma, Menas Saweha,

Ort: Hilton Vienna Plaza, Schottenring 11, 1010 Wien

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

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