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

April 2026 Ausgabe Nr. 122

Liebe Leserinnen und Leser,

willkommen zu unserer neuen Ausgabe des DSG-Info Service.

Das Ende März stattgefundene Datenschutzseminar der Secur-Data war wieder ein spezielles Highlight. Das jährlich veranstaltete Seminar bot allen Teilnehmenden aktuelle Einblicke in Datenschutzthemen und jede Menge Möglichkeiten zur praxisnahen Diskussion. Unsere ExpertInnen teilten ihr Wissen mit den anwesenden Vertretern aus Wirtschaft, Verwaltung und Recht und brachten dabei zahlreiche praxisnahe Beispiele sowie Neues aus nationaler und europäischer Judikatur.

Unmittelbar vor der Publikation des Jahresberichts[1] des Europäischen Datenschutzausschusses für 2025 hat die österreichische Datenschutzbehörde Anfang April 2026 ihren Tätigkeitsbericht für 2025 veröffentlicht, Näheres dazu in dieser Ausgabe des DSG-Info Service. Ergänzend dazu hat die Behörde Mitte März 2026 nochmals bestätigt, dass sie sich auch heuer – wie bereits angekündigt – an der koordinierten Maßnahme des Europäischen Datenschutzausschusses, mit dem diesjährigen Fokus auf Transparenz- und Informationsverpflichtungen unter der DSGVO, beteiligen wird.

Ansonsten finden Sie in dieser Ausgabe einen Beitrag zum aktuellen Bericht des Europäischen Datenschutzausschusses zum Thema Löschung, Neuigkeiten zum Digitalen Omnibus sowie Berichte zur datenschutzrelevanten Judikatur mit Empfehlungen für den beruflichen Alltag.

Wir wünschen eine angenehme Lektüre!

Mag. Judith Leschanz
Geschäftsführung

1. Bericht des Europäischen Datenschutzausschusses zur europaweiten Aktion zur Umsetzung des „Recht auf Löschung“

Allgemeines

Der Europäische Datenschutzausschuss (EDSA) hat 2025 eine Umfrage zum Thema der Umsetzung des „Recht auf Löschung“ für personenbezogene Daten durchgeführt. Die entsprechenden Ergebnisse dieser Umfrage sind in einem Bericht[2] zusammengefasst, welcher Ende Februar 2026 veröffentlicht wurde.

Der EDSA hatte im Laufe des Jahres 2025 an insgesamt 32 europäische Aufsichtsbehörden

[1] https://kurzlinks.de/amtm
[2] https://kurzlinks.de/p6aq

sowie an 764 Unternehmen und sonstige Verantwortliche einen Fragebogen zum Thema Löschung versandt, um durch die Antworten Erkenntnisse zu gewinnen und entsprechende Empfehlungen abzuleiten.

Unter den befragten Behörden und Unternehmen ist die datenschutzkonforme Einhaltung der Löschanforderungen laut Umfrage einerseits abhängig von der Größe und dem Sektor bzw. der Branche des Unternehmens. Andererseits sind auch die Anzahl der eingehenden Löschersuchen, die Verarbeitungsvorgänge sowie die unterschiedlichen Kategorien personenbezogener Daten beim Thema Löschung von Bedeutung.

Besondere Herausforderungen bestehen für die befragten Verantwortlichen dabei u.a. durch den (häufigen) Mangel an klaren internen Regelungen und Schulungen zu diesem Thema sowie die Weitergabe der Informationen an Betroffene.

Oft treten Rechtsunsicherheiten im Zusammenhang mit Ausnahmetatbeständen und den geltenden Aufbewahrungsfristen auf. Weiters sehen die befragten Unternehmen auch vielfach Unklarheiten bei der Löschung von Daten aus Backups und bezüglich der Anforderungen an die Anonymisierung der Daten.

Der EDSA äußert sich im Bericht schließlich zum Thema der Löschung aus Datensicherungen und hält dazu fest, dass es nicht immer ratsam ist, Daten aus Backups zu löschen. Dies ist insbesondere im Fall von Cyberangriffen wie zB Ransomware-Attacken kritisch, da Daten in derartigen Fällen oftmals wiederherzustellen sind und dies nach einer erfolgten Löschung aus Backup-Systemen nicht möglich ist.

Der Bericht des EDSA enthält abschließend einige Empfehlungen zum Thema Löschung, sowohl für Verantwortliche als auch für Aufsichtsbehörden bei ev. Prüfungen von Verantwortlichen.

Fazit

Der Bericht des EDSA zeigt deutlich, welche Schwierigkeiten regelmäßig mit dem Thema Löschung, insbesondere bei der praktischen Umsetzung, bestehen. Es zeigt sich, wie essentiell klare und gut kommunizierte interne Regelungen, inklusive Schulungen, zur Vermeidung von Problemen bei der Löschung sind.

Auch sollten Unternehmen jedenfalls bei Backups verstärkt auf (eventuell) noch benötigte Daten als Teil ihrer Informationssicherheitsstrategie im Fall von Angriffsszenarien achten.

2. Rückblick auf das Datenschutz-Seminar 2026

Das im März 2026 stattgefundene Datenschutzseminar der Secur-Data bot wie jedes Jahr allen teilnehmenden ExpertInnen und Mitarbeitenden umfassende Weiterbildung im Bereich des Datenschutzes und deckte dabei Theorie und Praxis gleichermaßen ausführlich ab.

Dabei richtete sich die Veranstaltung an Datenschutzbeauftragte und -koordinatorInnen, JuristInnen, ExpertInnen im Bereich der IT, UnternehmensberaterInnen sowie Compliance- und Sicherheitsbeauftragte.

Seminarinhalte

Die Veranstaltung vermittelte in zwei verschiedenen Modulen umfassenden Überblick über aktuelle Entwicklungen im Datenschutz sowie deren praktische Umsetzung in Unternehmen.

Am ersten Seminartag standen die rechtlichen Grundlagen der DSGVO im Fokus, ergänzt durch aktuelle Fälle der nationalen und internationalen Rechtsprechung. Behandelt wurden zentrale Themen wie Auskunftsrechte, Videoüberwachung, Konzern-Datenverarbeitung, Internationaler Datenverkehr sowie der

Umgang mit Datenschutzverletzungen. Auf die rechtlichen Anforderungen im Bereich des Arbeitsrechts sowie im Online-Marketing wurde genauso intensiv eingegangen wie auf neue Regulierungen mit Datenschutzbezug, insb. den Digitalen Omnibus der EU.

Ein Vertreter der Datenschutzbehörde gab zusätzlich detaillierte Einblicke in die Tätigkeit der Behörde und berichtete über die aktuellen Herausforderungen sowie jüngsten Entscheidungen der Datenschutzbehörde.

Der zweite Tag konzentrierte sich auf die Umsetzung von Datenschutzthemen in der Praxis. Die Teilnehmenden erhielten konkrete Anleitungen zum Aufbau eines Datenschutzmanagementsystems, zur Durchführung von Risiko- und Gap-Analysen sowie zur Implementierung von Sicherheitsmaßnahmen. Weitere Schwerpunkte waren der Check von Websites und der datenschutzkonforme Einsatz von Künstlicher Intelligenz und Cloud-Lösungen.

Ergänzend zu den SpezialistInnen von Secur-Data trug Mag. Krzysztof Müller, Berater und Experte auf dem Gebiet der Informationssicherheit, über Aspekte der Datensicherheit vor und nannte dabei zahlreiche konkrete Beispiele zur Umsetzung in der Praxis.

Fazit

Die unzähligen Diskussionen während des Seminars verdeutlichten den interaktiven Charakter der Veranstaltung. Die vielen positiven Rückmeldungen der Teilnehmenden, ebenso wie vereinzelte Wünsche nach einer dreitägigen Veranstaltung, zeigen den Erfolg des Seminars und unterstreichen dabei die zentrale Bedeutung der Wissensvermittlung zum Aufbau und der Weiterentwicklung einer gut geplanten und durchdachten Datenschutzstrategie, speziell im Bereich der Künstlichen Intelligenz, für Unternehmen aus unterschiedlichsten Branchen.

••••

Save the Date – Datenschutzseminar

Gerne kündigen wir Ihnen unser nächstes jährliches Datenschutz-Praxisseminar am **16. und 17. März 2027** im Hilton Vienna Plaza an. In unserem bewährten Seminar vermitteln wir den neuesten Stand von Recht und Technik, indem wir auf aktuelle Entwicklungen, Rechtsprechung und Praxisbeispiele eingehen.

Wir freuen uns auf Ihre Anmeldung - telefonisch unter (01) 533 42 07-0 oder hier.

3. Tätigkeitsbericht 2025 der Österreichischen Datenschutzbehörde

Die Österreichische Datenschutzbehörde (DSB) hat gemäß § 23 Datenschutzgesetz (DSG) jährlich bis zum 31. März einen Tätigkeitsbericht (bisher „Datenschutzbericht“) gemäß Art. 59 DSGVO zu erstellen, dem Bundesministerium für Justiz vorzulegen und zu veröffentlichen.

Die DSB hat nunmehr am 8. April 2026 ihren Tätigkeitsbericht[3] für das Jahr 2025 veröffentlicht.

Darin betont die DSB einmal mehr die Vielzahl der Herausforderungen der Behörde vor dem Hintergrund von Budgetkürzungen und Personalverknappungen, insbesondere durch eine massive Zunahme der – häufig auf Rechtsmissbrauch basierenden – Beschwerdeverfahren.

2025 gab es mit insgesamt 5.300 Beschwerden (nach 3019 Beschwerden in 2024) einen erheblichen Anstieg bei der Anzahl der Individualbeschwerden. Dies ist insbesondere auch auf die KI-unterstützte Erstellung von Beschwerden unter Zuhilfenahme von sog. Large Language Models (zB ChatGPT) zurückzuführen, wodurch laut DSB „erhebliche Ressourcen“ gebunden werden.

Wie bereits in den Jahren davor stiegen auch 2025 die Meldungen von Datenschutzvorfällen an. Insgesamt wurden 1.855 Sicherheitsverletzungen (nach 1.319 Sicherheitsverletzungen 2024) gemeldet und es kam zu 1804 entsprechenden Erledigungen durch die DSB (2024: 936 Erledigungen). 1.704 Meldungen waren dabei „Data Breaches“ gemäß Art. 33 DSGVO, 68 Meldungen betrafen grenzüberschreitende Verletzungen und 83 Sicherheitsverletzungen gab es in der Telekommunikationsbranche.

Der Großteil des Datenschutzverletzungen erfolgte laut Behörde aufgrund von Hacking-Angriffen sowie Ransomware-Attacken.

Auch werden im Tätigkeitsbericht wie gewohnt einige Entscheidungen der DSB, des BVwG sowie höchstgerichtliche Entscheidungen über datenschutzrechtliche Themen aus dem letzten Jahr angeführt. Vorrangig ist hier das Erkenntnis des VwGH[4] – aufgrund des EuGH-Urteils vom 9. Jänner 2025 (C-416/23) – zur Ablehnung einer Beschwerde gemäß Art. 57 Abs. 4 DSGVO aufgrund Exzessivität mit Voraussetzung des Nachweises einer Missbrauchsabsicht von besonderer praktischer Relevanz.

Im weiteren Verlauf des Berichts geht die Behörde auf ihre zusätzlichen Aufgaben aufgrund diverser (neuer) Rechtsvorschriften ein. Seit Inkrafttreten des Informationsfreiheitsgesetzes[5] Ende September 2025 wurden in Summe 8.236 Anträge auf Zugang zu Informationen an die DSB als informationspflichtiges Organ gestellt. Von den großteils durch die Bundes- bzw. Landesverwaltung und Gemeinden gemeldeten Anträgen wurden 404 Anträge mit Bescheid erledigt.

Der Tätigkeitsbericht der DSB enthält weiters Details zur KI-VO, speziell zur „teils zwingend, teils fakultativen“ Rolle der DSB als Grundrechts- sowie Marktüberwachungsbehörde nach der KI-VO.

Außerdem äußert sich die DSB zur „Verordnung über Transparenz und das Targeting politischer Werbung“,[6] da sie als Aufsichtsbehörde für die Überwachung und Durchsetzung dieser Verordnung zuständig ist.

---

[3] https://kurzlinks.de/q7k2

[4] VwGH-Erkenntnis vom 29. Jänner 2025, Ra 2023/04/0002

[5] Bundesgesetz über den Zugang zu Informationen (Informationsfreiheitsgesetz – IFG), BGBl. I Nr. 5/2024, in Kraft seit 1.9.2025

[6] VO (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung.

Schließlich informiert die Behörde über ihre Zuständigkeit im Zuge der Richtlinie zur Plattformarbeit.[7] Der DSB werden dabei umfassende Aufgaben bei Vollzug sowie Einhaltung der Umsetzung des noch zu beschließenden Bundesgesetzes im Rahmen der Umsetzung der EU-Richtlinie zugeteilt.

Schließlich wirft Behördenleiter Dr. Schmidl noch einen Blick auf das Jahr 2026, welches „richtungsweisende Änderungen" bringen soll, womit u.a. eine etwaige bereits diskutierte Novelle des Datenschutzgesetzes insb. zum Thema Verfahrensbeschleunigung in Aussicht gestellt wird.

4. Aktuelles zum Digitalen Omnibus

Wie bereits in DSG-Info-Service Nr. 120 und DSG-Info-Service Nr. 121 zu den seit November 2025 vorliegenden Plänen für den sog. **„Digitalen Omnibus"** – mit Änderungen zum Data Act sowie der DSGVO in Teil 1,[8] und Änderungen zum AI Act[9] in Teil 2[10] – berichtet, nimmt der Digitale Omnibus weiter Fahrt auf.

Dieser Digitale Omnibus ist Teil eines insgesamt zehn Bereiche umfassenden Omnibus-Gesamtpakets[11] der EU, welches zur Vereinfachung, Deregulierung sowie Stärkung der Wettbewerbsfähigkeit der EU und der Wirtschaft beitragen soll.

Die beiden Europaabgeordneten **Michael McNamara** und **Arba Kokalari wurden** zu **Berichterstattern für das „AI Omnibus"-Paket** (Änderungen zum AI Act) ernannt.

Das Europäische Parlament hat nunmehr am 26. März 2026 seine endgültige Verhandlungsposition[12] zum AI Omnibus-Paket, speziell zur Verschiebung diverser Verpflichtungen für Hochrisiko-KI-Systeme aus dem AI Act, angenommen.

Für alle ausdrücklich im AI Act angeführten Hochrisiko-KI-Systeme (einschließlich jener im Bereich Biometrie sowie Systeme, die in kritischen Infrastrukturen, Bildung, Beschäftigung, wesentlichen Dienstleistungen, Strafverfolgung, Justiz und Grenzmanagement eingesetzt werden) schlagen die Abgeordneten des Europäischen Parlaments nunmehr den 2. Dezember 2027 (anstatt des aktuell gültigen Termins 2. August 2026) als Anwendungsdatum vor.

Für KI-Systeme, die unter sektorspezifische EU-Rechtsvorschriften zu Sicherheit und Marktüberwachung fallen, sollen die Vorschriften des AI Act erst ab 2. August 2028 (anstatt 2. August 2027) gelten, um dadurch mehr Vorhersehbarkeit und Rechtssicherheit zu gewährleisten.

Als nächster Schritt zur Umsetzung des AI-Omnibus folgen jetzt im Zuge des sog. „Trilogverfahrens" Verhandlungen mit dem Rat der Europäischen Union, welcher seine Verhandlungsposition am 13. März 2026 angenommen hat, sowie mit der Europäischen Kommission.

Ziel ist es, während der Ratspräsidentschaft Zypern bis Ende Juni 2026 die ratsinternen Verhandlungen sowie den finalen Text zum AI-Omnibus abzuschließen.

Über weitere Entwicklungen zum „Digitalen Omnibus" werden wir Sie jedenfalls auf dem Laufenden halten.

---

[7] Richtline (EU) 2024/2831 vom 23. Oktober 2024 zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit

[8] https://kurzlinks.de/y1xu

[9] https://kurzlinks.de/oflw

[10] https://kurzlinks.de/ict0

[11] https://kurzlinks.de/s25m

[12] https://kurzlinks.de/oy0c

Beratung im Bereich Künstliche Intelligenz: KI-Strategie

Aktuelle Studien zeigen es deutlich:

- 4 von 10 Unternehmen scheitern an KI-Strategie
- Jedes zweite Unternehmen in Österreich hat keine KI-Strategie
- Schatten-KI in Unternehmen wird zum Sicherheitsrisiko

Wo steht IHR Unternehmen?

Unser Angebot, um Sie mit KI erfolgreicher zu machen:

Schritt 1: Bestandsaufnahme / KI-Check

- ✓ Prüfung aktuell eingesetzter Tools auf Compliance mit DSGVO und AI Act
- ✓ Rollendefinition: KI-Anbieter vs. KI-Betreiber, Verantwortlicher vs. Auftragsverarbeiter

Schritt 2: Entwicklung einer internen KI-Strategie

- ✓ Erstellung einer unternehmensinternen KI-Strategie zum erfolgreichen Einsatz von KI im Unternehmen
- ✓ Bereitstellung von KI-Handbüchern, um den datenschutzkonformen Einsatz von KI sicherzustellen
- ✓ Durchführung einer detaillierten Risikobewertung
- ✓ Schulung und Sensibilisierung von Mitarbeitern und Führungskräften

Schritt 3: Umsetzung

- ✓ Weiterentwicklung der eingesetzten Tools im Rahmen der KI-Strategie
- ✓ Unterstützung bei Auswahl, Compliance-Bewertung und Umsetzung neuer KI-Systeme
- ✓ Unterstützung bei Festlegung und Prüfung von Use-Cases für den KI-Einsatz
- ✓ Erstellung geeigneter Vorlagen zur Erfüllung der rechtlichen Anforderungen gegenüber Kunden und Behörden
- ✓ KI-Register: Vollständige unternehmensinterne Übersicht aller KI-Anwendungen
- ✓ Weiterentwicklung der KI-Kompetenz durch regelmäßige Schulungen und Workshops
- ✓ KI-Audit: Regelmäßige Überprüfung des KI-Einsatzes

Kontaktieren Sie uns jetzt für Ihr individuelles Angebot!

5. EuGH-Urteil vom 19. 3. 2026, C-526/24 „Brillen Rottler“

Der Europäische Gerichtshof (EuGH)[13] entschied im März 2026 zu exzessiven bzw. rechtsmissbräuchlichen Auskunftsersuchen und zur Frage des Ersatzes von immateriellem Schaden

Sachverhalt

Eine Person verlangte, nachdem sich diese beim Newsletter eines Optikers in Deutschland angemeldet hatte, von diesem eine Auskunft nach Art. 15 DSGVO. Der Optiker verweigerte die Auskunft mit dem Verweis auf Rechtsmissbrauch des Auskunftsersuchens. Die Person verlangte daraufhin in einem erneuten Auskunftsersuchen zusätzlich immateriellen Schadenersatz iHv EUR 1.000 vom Optiker. Der Optiker brachte beim zuständigen Gericht eine Feststellungsklage ein, da die betroffene Person, wie aus öffentlichen Quellen ersichtlich war, systematisch mit ähnlichen Auskunftsersuchen gegen mehrere Verantwortliche und somit rechtsmissbräuchlich vorgegangen war.

Das Amtsgericht Amsberg legte dem EuGH in weiterer Folge die **Fragen zur Exzessivität von Auskunftsersuchen** nach Art. 12 Abs. 5 DSGVO sowie zur Ersatzfähigkeit des Schadens nach Art. 82 Abs. 1 DSGVO zur Vorabentscheidung vor.

Entscheidungsgründe

Der EuGH entschied erstmalig zur Frage der Exzessivität von Auskunftsersuchen an Verantwortliche nach Art. 12 Abs. 5 DSGVO und dehnte in der Entscheidung die bereits im Fall *„Österreichische Datenschutzbehörde“* vom 9. Jänner 2025[14] getroffenen Feststellungen zu exzessiven Anfragen auch auf Anfragen an Verantwortliche nach Art. 12 Abs. 5 DSGVO aus.

Laut EuGH sind für das Vorliegen einer Exzessivität bzw. eines Rechtsmissbrauchs eines Auskunftsersuchens nach Art. 12 Abs. 5 DSGVO nicht die Anzahl, sondern **qualitative Kriterien ausschlaggebend**. Es kann daher auch ein nur einmaliges Auskunftsersuchen unter Umständen bereits rechtsmissbräuchlich sein. Für die Beurteilung sind die **Maßstäbe** dabei **sehr hoch** anzusetzen und gemäß EuGH sowohl **objektive Umstände als auch subjektive Elemente** heranzuziehen.

Das **relevante Kriterium** für Rechtsmissbrauch ist immer der **zugrundeliegende Zweck** des Ersuchens. Ein solches liegt laut EuGH insb. dann vor, wenn ein Betroffener **„künstlich“ die Voraussetzungen für Schadenersatz schafft**.

Dass der Betroffene sich nach Einwilligung in die Verarbeitung mit Auskunftsersuchen inkl. Schadenersatzforderung **systematisch** an verschiedene Verantwortliche gewandt hat, ist laut EuGH ein **„Anhaltspunkt“** für einen Rechtsmissbrauch. Jedoch ist immer eine **Einzelfallprüfung notwendig** und der Verantwortliche hat diesen Rechtsmissbrauch in jedem Fall nachzuweisen.

Weiters befasste sich der EuGH mit der Frage der **Ersatzpflicht von immateriellem Schaden**. Für die Forderung nach immateriellem Schadenersatz ist es laut EuGH jedenfalls notwendig, einen **tatsächlichen Schaden** nachzuweisen.

Dabei genügt es nicht, dass ein Betroffener sich nur auf den „Verlust der Kontrolle“ über die personenbezogenen Daten bezieht. Es ist vielmehr ein **Kausalzusammenhang zwischen Verstoß und Schaden** nachzuweisen. Dies ist jedenfalls nicht gegeben, wenn der Betroffene

[13] https://kurzlinks.de/llr9

[14] EuGH 9.1.2025, C-416/23 https://kurzlinks.de/8prv

selbst durch eigene Entscheidung den Kontrollverlust „künstlich“ verursacht.

Fazit

Durch dieses Urteil des EuGH wird einerseits eine **längst überfällige Klarstellung** im Zusammenhang mit Auskunftsersuchen an Verantwortliche getroffen.

Andererseits ist diese **Entscheidung** insb. vor dem Hintergrund der zunehmenden Anzahl an gestellten Auskunftsersuchen als **richtungsweisend** anzusehen.

Dadurch wird für die quer durch alle Branchen steigende „Überflutung“ mit oftmals unpassenden, zweckwidrigen, **fern von datenschutzrechtlichen Motiven** und somit häufig offenkundig missbräuchlich gestellten Auskunftsersuchen Rechtssicherheit und Klarheit für die (mögliche) Abweisung geschaffen.

Vor dem Hintergrund dieser EuGH-Entscheidung sollten Unternehmen ihre **internen Prozesse zur Auskunftserteilung optimieren** und gegebenenfalls anpassen, um künftig klar rechtsmissbräuchlich gestellten Auskunftsersuchen, insb. wenn damit weitere rechtliche Schritte angekündigt werden, entgegenwirken zu können.

6. Verwaltungsstrafen

Fall 1 - Bestätigung der durch die französische Datenschutzbehörde verhängten Geldbuße in Höhe von EUR 40 Mio.

In einem bereits seit 2023 anhängigen Verfahren der **französischen Datenschutzbehörde CNIL** gegen das Unternehmen **CRITEO** aufgrund einer Vielzahl an Datenschutzverstößen wurde nunmehr die in Höhe von EUR 40 Mio. verhängte Geldbuße durch das oberste Verwaltungsgericht (Conseil d'État) bestätigt.[15]

Sachverhalt

Die französische Datenschutzbehörde wurde ursprünglich aufgrund einiger Beschwerden von diversen Verbänden tätig.

Das Geschäftsmodell von CRITEO basiert darauf, dass die Navigation von Internetbenutzern mittels Tracking Cookies auf ihren Geräten überwacht und dadurch ihr Verhalten im Netz analysiert wird, um gezielte, personalisierte Werbung zu platzieren.

Das Unternehmen CRITEO, welches diese Online-Marketing-Maßnahmen durch ein eigenes Tracking-Tool anbietet, hatte argumentiert, dass die Daten durch starke Pseudonymisierung nicht mehr auf den einzelnen Benutzer rückführbar wären.

Nach genauer Prüfung stellte die CNIL fest, dass die Daten sehr wohl personenbezogen sind, wenn eine **Re-Identifizierung** auch **nach erfolgter Pseudonymisierung** möglich ist.

Weiters fand CNIL heraus, dass CRITEO sowohl **Tracking- als auch Tracer-Cookies oft ohne Einwilligung der Nutzer** platziert hatte und dabei versäumt hatte, zu prüfen, ob eine Einwilligung vorlag. Außerdem hatte CRITEO keinerlei technische Maßnahmen ergriffen, um zu prüfen bzw. sicherzustellen, dass die jeweiligen Website-Partner eine wirksame Einwilligung der Internetnutzer zur Verarbeitung der Daten eingeholt hatten.

Darüber hinaus hat CNIL bei CRITEO eine zu **unpräzise** formulierte **Datenschutzpolitik** festgestellt, es wurde das **Auskunftsrecht** von Betroffenen **nicht rechtskonform** erfüllt und es wurden beim Widerruf der Einwilligung und bei Löschersuchen die entsprechenden **Browser-**

[15] https://kurzlinks.de/7jglhttps://kurzlinks.de/7jgl

Kennungen nicht (vollständig) durch CRITEO **gelöscht**.

Schließlich wurden Mängel in den zwischen CRITEO und anderen Verantwortlichen abgeschlossenen **Vereinbarungen** zur Regelung der gemeinsamen Verantwortlichkeit nach **Art. 26 DSGVO** festgestellt. Laut französischer Aufsicht wurden in den Art. 26-Vereinbarungen einige **Pflichten sowie Anforderungen nicht** (ausreichend) **festgelegt**. Dies betraf vor allem die Ausübung der Betroffenenrechte, die Meldungen von Datenschutzvorfällen an Aufsichtsbehörden und Betroffene sowie die Durchführung der Datenschutz-Folgenabschätzung.

Die Höhe der Geldbuße rechtfertigte die CNIL insbesondere aufgrund der Tatsache, dass EU-weit **Daten** von rund **370 Mio. Internetbenutzern unrechtmäßig** durch CRITEO **verarbeitet** worden sind.

Fazit

Dieser Fall zeigt speziell für alle Unternehmen im Bereich des digitalen Marketings, wie wichtig eine **lückenlose datenschutzrechtliche Dokumentation**, insb. beim Abschluss von Vereinbarungen zur gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO ist.

Auch führt diese hohe Bußgeldentscheidung wieder die Grenzen derartiger Marketing-Modelle beim Einsatz von personalisierter Werbung vor Augen, wie dies bereits der EuGH in seiner Judikatur (zB C-604/22) ausgeführt hat.

Schließlich zeigt die Entscheidung gegen CRITEO eindrucksvoll, wie hoch die **Strafen bei Nichteinhaltung** der **datenschutzrechtlichen Vorschriften**, speziell bei Verletzung der Auskunfts- und Transparenzpflichten und Erfüllung der Betroffenenrechte sein können, und auch die möglichen **Auswirkungen auf Unternehmen**. So kam es rund um die Strafverhängung gegen CRITEO zu einem Einbruch des Aktienkurses und zu diversen Umstrukturierungsmaßnahmen des Unternehmens.[16]

Fall 2 – Aufhebung der durch die luxemburgische Datenschutzbehörde verhängten Geldbuße in Höhe von EUR 748 Mio.

In einem weiteren bedeutsamen Fall wurde die durch die **Luxemburgische Datenschutzbehörde** („Commission nationale pour la protection des données" – **CNPD**) verhängte Geldstrafe in Höhe von EUR 746 Mio. gegen **Amazon Europe Core S.à r.l** vom obersten Verwaltungsgericht in Luxemburg nunmehr aufgehoben.

Sachverhalt

In diesem aufsehenerregenden Fall aus 2021 wurde die bis dahin EU-weit höchste Geldbuße aufgrund von Verstößen gegen die DSGVO verhängt. 2023 wurde diese Geldbuße durch die von der irischen Datenschutzbehörde gegen Meta Platforms Ireland Limited (eh. Facebook) verhängte Strafe in Höhe von EUR 1,2 Mrd. übertroffen.

Die luxemburgische Aufsichtsbehörde stellte in ihrem Verfahren aus 2021 datenschutzrechtliche **Verstöße durch Amazon** bei der Verarbeitung personenbezogener Daten für **interessenbasierte Werbung** fest. Die Verstöße reichten von der **mangelnden Einholung der Einwilligung** der Nutzer (Art. 6 Abs. 1 lit. a DSGVO) über die **Verletzung der Transparenz- und Informationspflichten** (Art. 12, 13 DSGVO) und des **Rechts auf Zugang** zu den verarbeiteten Daten (Art. 15 DSGVO), der **Verletzung des Rechts auf Berichtigung und Löschung** der verarbeiteten, personenbezogenen Daten (Art. 16, 17 DSGVO) bis zur **Verletzung des Rechts auf Widerspruch** (Art. 21 DSGVO).

In einer Presseaussendung[17] im Juli 2021 zeigte ein Vertreter von Amazon offenkundig wenig Einsicht und erklärte öffentlich, dass es „keine Verletzung des Schutzes personenbezogener

[16] https://kurzlinks.de/29w2

[17] https://kurzlinks.de/zhn6

Daten gab, und es wurden keine Kundendaten an Dritte preisgegeben."

Im jetzigen Urteil des obersten Verwaltungsgerichts in Luxemburg wurden zwar die **Datenschutzverstöße durch Amazon bestätigt**, es wurden jedoch **Verfahrensmängel durch die CNPD** festgestellt.[18] Offenbar waren zentrale rechtliche Prüfungen durch die luxemburgische Aufsicht nicht durchgeführt worden. Auch hatte die CNPD unterlassen, vor der Verhängung der Geldbuße eine Prüfung bzgl. eines fahrlässigen und vorsätzlichen Verstoßes gegen die DSGVO, wie es Art. 83 Abs. 1 lit. b DSGVO vorsieht, durchzuführen.

Das Verfahren wurde zur neuerlichen Prüfung und Durchführung an die CNPD übergeben.

Fazit

Obwohl es in diesem Fall nach jahrelangem Rechtsstreit zur Aufhebung der Geldbuße gekommen ist, bleiben die Datenschutzverstöße dennoch unumstritten rechtswidrig und sind in jedem Fall zu vermeiden. Auch wenn gerichtlich ein (erster) Erfolg erzielt wurde, wie in diesem Fall von Amazon, sollten sich alle Unternehmen unabhängig von Größe und Branche dennoch aller datenschutzrechtlichen Verpflichtungen bewusst sein und diese einhalten.

••••

[18] https://kurzlinks.de/0qf9