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

November 2025 Ausgabe Nr. 119

Liebe Leserinnen und Leser,

Das Jahr 2025 nähert sich mit riesigen Schritten dem Ende – und wir bedanken uns bei Ihnen schon jetzt für die Zusammenarbeit.

Das Jahr brachte für Secur-Data ein großes Jubiläum: Wir feiern unser 50-jähriges Bestehen. 1975 wurde das Unternehmen von Hans-Jürgen Pollirer gegründet, übrigens im selben Jahr wie Microsoft! In diesen fünf Jahrzehnten hat sich der Datenschutz von einem Nischenthema zu einer vieldiskutierten Materie entwickelt, nicht zuletzt vor dem Hintergrund aktueller Herausforderungen wie dem Thema Künstliche Intelligenz.

Dass diese Herausforderungen im Datenschutz nicht weniger werden, zeigen neueste Entwicklungen auf EU-Ebene: Der sog. „Digitale Omnibus" der EU enthält einige zu erwartende Änderungen der EU-Datenschutz-Grundverordnung wie auch anderer EU-Rechtsakte. Wir werden Sie zeitnah über die genauen Details auf unserer Website informieren.

In dieser Ausgabe richtet sich unser Augenmerk auf die Tätigkeit der Österreichischen Datenschutzbehörde und ihre künftige Ausrichtung.

Auf der regulatorischen Seite betrachten wir den mit Mitte September 2025 in Kraft getretenen Data Act.

Schließlich finden Sie neben aktuellen und spannenden Entscheidungen aus der österreichischen Rechtsprechung wie gewohnt Auszüge aus Top-Bußgeldern für Datenschutzverstöße.

Wir wünschen Ihnen eine angenehme Lektüre und eine stressfreie Weihnachtszeit!

Mag. Judith Leschanz
Geschäftsführung

1. 50 Jahre Secur-Data

2025 ist ein Meilenstein für uns — **SECUR-DATA wird 50!**

Mit der **Gründung durch Prof. KommR Hans-Jürgen Pollirer** beginnt die Geschichte von Secur-Data als Beratungsunternehmen im Bereich Datenschutz und Informationssicherheit. Der Eintritt von **Mag. Judith Leschanz** 2017 und ihre **Übernahme der Geschäftsführung 2020** stärkte die fachliche Expertise weiter.

Viel hat sich seither getan: das erste österreichische Datenschutzgesetz 1978, der Beschluss der Europäischen Datenschutzrichtlinie 1995, die Einführung der EU-Datenschutz-Grundverordnung, die Umsetzung zahlreicher nationaler und EU-Regularien – jüngste Beispiele dafür sind NIS-2, das Informationsfreiheitsgesetz oder der Data Act – und der technische Fortschritt – Digitalisierung, Online-Angebote,

Social Media, bis hin zum aktuellen Thema Künstliche Intelligenz.

Wir standen in den letzten fünf Jahrzehnten vor einer **Vielzahl von Herausforderungen**, bei denen wir unsere Kunden laufend unterstützt und begleitet haben. Das Thema Datenschutz ist heute aktueller denn je und beschäftigt nicht nur Unternehmen intensiv, sondern wird auch in der Öffentlichkeit heiß diskutiert – sei es beim Thema Videoüberwachung, dem internationalen Datentransfer, den Rechten und Freiheiten des Einzelnen in der digitalen Welt oder der Datensicherheit. Dem rechtlichen und technischen Wandel entsprechend hat sich die Arbeit von Secur-Data stetig weiterentwickelt und das Beratungsangebot wurde laufend angepasst und verbessert.

Auch das **Team von Secur-Data** wurde erweitert und besteht sowohl aus **CIS-zertifizierten TechnikerInnen** als auch aus **juristischen ExpertInnen**. Das gesamte Team stellt aufgrund der vielfältigen Kenntnisse und Erfahrungen eine optimale Beratung für alle unsere Kunden sicher.

Aufgrund unserer **Erfahrung und fachlicher Expertise** sind wir für künftige Themen und Herausforderungen **bestens gerüstet** und starten voller Elan in die nächsten Jahre und Jahrzehnte.

Wir bedanken uns bei unseren Kunden und richten den Blick in die Zukunft, um diese gemeinsam zu gestalten!

2. Aktuelles von der Datenschutzbehörde

Aufgaben der Datenschutzbehörde aufgrund neuer gesetzlicher Vorschriften

Durch neue Regularien erhält die österreichische Datenschutzbehörde (DSB) aktuell und künftig einige zusätzliche Aufgabenbereiche.

Hinsichtlich des **Informationsfreiheitsgesetzes (IFG)**[1] – nähere Infos dazu siehe DSG-Info-Service Nr. 117 vom März 2025 – nimmt die DSB die Aufgabe der Beratung und Unterstützung aller informationspflichtigen Stellen bzgl. der datenschutzrechtlichen Rechtslage und Praxis (insb. der Rechtsprechung) wahr. Zu diesem Zweck erstellt die DSB insbesondere Anwendungshinweise und Anleitungen und bietet auch Schulungsmaßnahmen an.

Siehe dazu den Leitfaden zum IFG, diverse Rundschreiben der DSB zum IFG sowie die ergänzenden Informationen dazu auf der Website der DSB.[2]

Weiters ist die DSB für alle datenschutzrechtlichen Fragestellungen im Zusammenhang mit **Systemen Künstlicher Intelligenz** (sog. KI-Systeme) insbesondere vor dem Hintergrund des neuen **AI Acts**[3] – siehe dazu Näheres im DSG-Info-Service Nr. 116 vom Jänner 2025 – zuständig. Zusätzlich kommt ihr dabei die Funktion als Marktüberwachungsbehörde für KI-Systeme mit hohem Risiko u.a. im Bereich der Strafverfolgung, der Grenzverwaltung, der Justiz und der Demokratie (nach aktueller Rechtslage) gemäß § 18, § 31 DSG zu.

Schließlich erhielt die DSB die Aufgaben bzgl. der Aufsicht und Sanktionen im Zusammenhang mit der **Richtlinie zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit (RL 2024/2831)**.

Zukünftig wird die DSB auch Aufgaben im Zusammenhang mit dem **Bundesgesetz über die**

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

[2] https://dsb.gv.at/informationsfreiheitsgesetz/informationsfreiheitsgesetz

[3] Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Transparenz und das Targeting politischer Werbung nach dessen Verabschiedung übernehmen.

Schwerpunktprüfung 2025

Wie schon in den Jahren davor führte die DSB auch 2025 ein amtswegiges Prüfverfahren durch, in dem Unternehmen eines bestimmten Sektors einer vertieften Prüfung aus datenschutzrechtlicher Sicht unterzogen wurden.

Als zu prüfenden Sektor wählte die DSB für die amtswegige **Schwerpunktprüfung 2025** die **österreichischen Landespolizeidirektionen** aus. Dabei wurde einerseits die Einhaltung der Datenschutz-Grundverordnung (DSGVO) geprüft, andererseits die genaue Einhaltung des 3. Hauptstücks des Datenschutzgesetzes (DSG), mit dem die Richtlinie (EU) 2016/680 umgesetzt wurde.

Im Mittelpunkt des diesjährigen Prüfverfahrens standen die gesetzlich vorgeschriebenen **Dokumentationspflichten** und spezifisch datenschutzrechtlichen **Anforderungen bei der Verarbeitung von personenbezogenen Daten** im polizeilichen Bereich. Gemäß dem Rahmen des Coordinated Enforcement Frameworks (CEF) des Europäischen Datenschutzausschusses (EDSA) lag dieses Jahr ein zusätzlicher Prüfschwerpunkt auf der rechtlich korrekten **Umsetzung des Betroffenenrechts auf Löschung** sowie den entsprechenden Speicherfristen.

Nachdem das Prüfverfahren beendet wurde, verkündete die Datenschutzbehörde kürzlich das Ergebnis des Verfahrens. Beim diesjährigen Schwerpunktverfahren gab es aus Sicht der DSB **keine Beanstandungen**. Das Ergebnis bestätige laut DSB, dass die Verantwortlichen im polizeilichen Bereich den Datenschutz nicht nur ernst nehmen, sondern auch in der praktischen Umsetzung wirksam gewährleisten.

Zukünftige Schwerpunktprüfungen

Auch im kommenden Jahr wird die DSB amtswegige Prüfverfahren durchführen. Diese Verfahren werden jedoch einen anderen Ablauf haben als die bisherigen Schwerpunktprüfungen. **2026** wird die DSB erstmals **Schwerpunktprüfungen** im Sinne einer Jahresstrategie **ohne Bekanntgabe einer spezifischen Branche** oder eines Sektors durchführen. Zu diesem Zweck wird die DSB im Jänner 2026 die aktuellen Prüfungsschwerpunkte inklusive Bekanntgabe des Starts der Prüfung verkünden.

Künftige Positionierung der Datenschutzbehörde

Die notwendigen Einsparungsmaßnahmen im Bund treffen auch die Österreichische Datenschutzbehörde. In diesem Zusammenhang verkündete die DSB, dass die **geplanten Einsparungen** bereits ab Mitte 2025 Auswirkungen auf ihre Tätigkeit haben. Die Behörde hat dazu Maßnahmen im Zuge eines „contingency planning“ ergriffen. Die Verknappung der Personalressourcen wirkt sich auf die Wahrnehmung all ihrer Funktionen aus und macht daher eine klare Schwergewichtsbildung notwendig.

Konkrete Änderungen im Arbeitsablauf der Datenschutzbehörde

Die DSB nimmt, um weiterhin allen Pflichten nachkommen zu können, intern u.a. folgende Änderungen vor:

- Der **Schwerpunkt** der Tätigkeit der DSB wird weiterhin auf der **Bearbeitung von Beschwerden** liegen, da in diesem Bereich eine gesetzliche Behandlungspflicht besteht und dadurch dem subjektiven Recht der Betroffenen auf Behandlung der Beschwerden entsprochen wird. Verzögerungen bei der Bearbeitung werden laut DSB jedoch unvermeidbar sein.
- Künftig wird die DSB **amtswegige Prüfverfahren** nur noch dann einleiten, wenn sich aus der Eingabe ein **hinreichend konkreter Verdacht** auf eine schwerwiegende datenschutzrechtliche Verletzung der DSGVO oder des DSG ableiten lässt.

- Bei **Data Breach-Meldungen nach Art. 33 DSGVO** wird künftig nur noch dann eine Mitteilung an den Verantwortlichen ergehen, wenn die DSB entweder Folgemaßnahmen für erforderlich hält oder die Meldung als unvollständig ansieht.
- Weiters schränkt die DSB u.a. ihre Erreichbarkeit, die Erteilung schriftlicher Rechtsauskünfte, die Teilnahme an Veranstaltungen, die Teilnahme an Sitzungen der EDSA-Untergruppen sowie Stellungnahmen in gesetzlichen Begutachtungsverfahren ein.

3. Der neue Data Act

Die **Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung**[4], der sog. Data Act, trat mit 11. Jänner 2024 in Kraft und ist seit 12. September 2025 anwendbar. Der Data Act regelt generell die Zugänglichkeit und Nutzung von Daten und stellt klar, unter welchen Bedingungen Daten einen Mehrwert schaffen.

Betroffen vom Data Act sind Daten, die von verbundenen Produkten („**Internet of Things"-IoT**) generiert und von privaten Akteuren gehalten werden. Beispiele für sog. IoT finden sich in der Landwirtschaft, bei Smart-Home-Geräten oder in der Medizintechnik. Dabei sind sowohl personenbezogene als auch nicht personenbezogene Daten umfasst.

Der Data Act stellt darüber hinaus sicher, dass

- der Nutzen von Daten fair verteilt wird,
- ein wettbewerbsfähiger EU-Datenmarkt entsteht,
- Innovationsmöglichkeiten gefördert werden,
- der Zugang zu Daten, insbesondere aus vernetzten Produkten, verbessert wird.

Adressaten

Der Data Act gilt für **Hersteller und Anbieter** von verbundenen Produkten, für zugehörige Dienste und Anbieter von Datenverarbeitungsdiensten, die im EU-Markt tätig sind und spricht dabei von **Nutzern, Dateninhabern und Datenempfängern**.

Als **Nutzer** gilt der Eigentümer eines verbundenen Produkts oder jemand, dem vertraglich Nutzungsrechte übertragen wurden.

Als **Dateninhaber** gilt eine juristische oder natürliche Person, die das Recht oder die Pflicht hat, Daten zu nutzen und verfügbar zu machen (zB der Hersteller des verbundenen Produkts oder der Anbieter des zugehörigen Dienstes, die in der EU in Verkehr gebracht werden).

Inhalt

Ziel des Data Acts ist der **faire Datenzugang** und die geregelte **Nutzung der Daten**. Dies wird u.a. erreicht durch die klare Regelung der Nutzungsrechte zur Datenweitergabe an Dritte, Schutz von Geschäftsgeheimnissen und geistigem Eigentum sowie Schutz vor unrechtmäßigem Zugriff Dritter auf nicht-personenbezogene Daten.

Rahmenbedingungen für die Nutzung von **Daten aus IoT-Geräten** werden dabei genauso wie das Verbot der Nutzung der Daten zur Entwicklung von konkurrierenden Geräten festgelegt. Auch sollen Anreize für Investitionen in qualitativ hochwertige Daten gesetzt sowie eine Förderung des sicheren und verlässlichen Zugangs zu Daten erreicht werden.

Durch den **Schutz vor unfairen Klauseln** werden faire Vertragsbedingungen geschaffen und

[4] Verordnung (EU) 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung

KMUs vor marktmächtigen Akteuren geschützt. Öffentliche Stellen erhalten nur im Notfall Zugang zu privaten Daten.

Effiziente Dateninteroperabilität stellt der Data Act genauso sicher wie den erleichterten Wechsel zwischen Datenverarbeitungsdiensten und Cloud-Anbietern, indem etwa die Wechselgebühren im Cloud-Bereich stufenweise abgeschafft werden. Außerdem fördert der Data Act gemeinsame europäische Datenräume.

Verhältnis von Data Act zu DSGVO

Vom Data Act umfasst sind sowohl **personenbezogene als auch nicht personenbezogene Daten**. Art. 1 Abs. 5 Data Act regelt ausdrücklich, dass im Falle eines Widerspruchs zwischen Data Act und DSGVO in Bezug auf den Schutz personenbezogener Daten die DSGVO jedenfalls Vorrang hat. Auch findet sich in ErwGr 7 zum Data Act die Verpflichtung, dass die DSGVO weder eingeschränkt noch abgeschwächt werden darf.

4. Neues aus der Rechtsprechung

Entscheidung der Datenschutzbehörde zur Nutzung von Microsoft 365 Education an einer Schule

Eine erst kürzlich getroffene Entscheidung der österreichischen Datenschutzbehörde (DSB)[5] befasst sich mit dem Einsatz der Software Microsoft 365 Education an einer österreichischen Schule. Diese Software dient u.a. dem IT-gestützten Unterricht und umfasst diverse Microsoft-Produkte.

Ausgangspunkt war ein Auskunftsersuchen des Vaters einer Schülerin an Microsoft, das von Microsoft jedoch mit Verweis, sich an die lokale Schule zu wenden, nicht beantwortet wurde. Die daraufhin kontaktierte Schule konnte nur minimale Auskünfte liefern und verwies diesbezüglich wiederum auf Microsoft.

Schließlich erhob der Vater, vertreten durch NOYB, Beschwerde bei der DSB, und zwar gegen die betroffene Schule, die zuständige Bildungsdirektion, das Bildungsministerium und auch gegen Microsoft.

Die DSB befasste sich zunächst mit der Frage der Verantwortlichkeit und der Rollen aller involvierten Stellen. Die Schule und das Bildungsministerium wurden als gemeinsam Verantwortliche gemäß Art. 26 DSGVO eingestuft und sind zur Erfüllung der Betroffenenrechte verpflichtet.

Zum Verhältnis zwischen Microsoft USA und Microsoft Ireland stellte die DSB fest, dass Microsoft USA die grundsätzlichen Entscheidungen über den Microsoft-Konzern trifft und vor allem auch Einfluss auf die Datenverarbeitung nimmt, indem sie u.a. das Produkt weiterentwickeln. Dadurch übt Microsoft USA den maßgeblichen Einfluss aus, ist daher als Verantwortlicher nach Art. 4 Z 7 DSGVO anzusehen und zur Auskunftserteilung verpflichtet.

Weiters stellte die DSB fest, dass bei der Nutzung von Microsoft 365 Education Tracking-Cookies ohne Einholen der Einwilligung und somit unrechtmäßig gesetzt wurden. Diesbezüglich ordnete die DSB die Löschung der in den Cookies enthaltenen Daten an.

Außerdem befand die Behörde, dass unklar ist, welche Daten Microsoft verarbeitet und auf welcher Rechtsgrundlage sowie zu welchen konkreten Zwecken die Daten verarbeitet werden. Offenbar wurden von Microsoft auch Daten an Drittanbieter (zB LinkedIn, OpenAI oder Xandr) weitergegeben, worüber es weder eine Auskunft noch genauere Informationen für Betroffene gab.

[5] DSB 08.10.2025, GZ: D135.027 2025-0.477.534

Aufgrund der getroffenen Feststellungen stellte die DSB einen Verstoß gegen die Informationspflichten nach Art. 13 DSGVO sowie eine Verletzung des Auskunftsrechts nach Art. 15 DSGVO fest.

Die DSB hat nunmehr der betroffenen Schule und dem Bildungsministerium den Auftrag zur korrekten Auskunftserteilung nach Art. 15 DSGVO sowie zu vollständigen Informationsbereitstellung, insbesondere hinsichtlich der Cookies, nach Art. 13 DSGVO erteilt. Microsoft USA wurde aufgetragen, über sämtliche personenbezogenen Daten Auskunft zu erteilen, inklusive der Datenübermittlung an Drittanbieter. Insbesondere hat Microsoft die Zwecke der Datenverarbeitung in der Auskunftserteilung gemäß Art. 12 Abs. 1 DSGVO „verständlich zu beschreiben".

Entscheidung des Obersten Gerichtshofs im Zusammenhang mit KI-Systemen

Vor kurzem hat der Oberste Gerichtshof (OGH) in einer Entscheidung[6] erstmals über die Verwendung von KI-Systemen für die Erstellung von Schriftsätzen entschieden.

Dabei wurde eine Nichtigkeitsbeschwerde gegen ein Urteil des Landesgerichts für Strafsachen Graz zurückgewiesen. Als Begründung stellte der OGH u.a. fest, dass der Inhalt des Schriftstücks mit Fehlzitaten übersät war und sich sowohl auf nicht korrekte Verfahrensergebnisse als auch auf nichtexistierende Urteile des OGH bezog. Dies lag laut OGH daran, dass der eingebrachte Schriftsatz offenbar durch die Verwendung von „Künstlicher Intelligenz" erstellt wurde und in weiterer Folge nicht fachlich kontrolliert wurde. Das Vorbringen „genügt dem Erfordernis, Nichtigkeitsgründe deutlich und bestimmt zu bezeichnen, also einen Nichtigkeit begründenden Sachverhalt auf einem dem Obersten Gerichtshof als Höchstgericht angemessenen Argumentationsniveau … nicht ansatzweise".

Anhand dieser Entscheidung zeigt sich, wie wichtig die Sensibilisierung, Weiterbildung und Bewusstseinsbildung beim Einsatz von KI-Systemen insbesondere im juristischen Kontext ist. Zwar bietet ihr Einsatz in der täglichen Arbeit viele Möglichkeiten und bringt vielerorts Erleichterungen, dennoch müssen die zahlreichen Schwachstellen bei den Ergebnissen, insb. durch sog „Halluzinationen", „Bias" und die „Black-Box"-Thematik (Intransparenz der Entscheidungen), immer bedacht werden. Bei diversen Fällen aus den USA zeigten sich bereits die Gefahren durch „Halluzinationen" von KI-Systemen im Zusammenhang mit Gerichtsentscheidungen.

Wesentlich ist daher, dass der Vorschlag eines KI-Systems keinesfalls ohne ausführliche Prüfung und Kontrolle durch einen Menschen verwendet werden darf und Bewusstsein über die Chancen, aber auch Grenzen des Einsatzes von KI-Systemen in jedem Unternehmen geschaffen wird.

Entscheidung des Bundesverwaltungsgerichts zu Videoüberwachung

Das Bundesverwaltungsgericht (BVwG) hat in einer Anfang Oktober 2025 veröffentlichten Entscheidung[7] eine von der Datenschutzbehörde verhängte Geldbuße gegen ein Handelsunternehmen bestätigt.

Aufgrund einer anonymen Anzeige leitete die Datenschutzbehörde (DSB) Anfang März 2022 ein amtswegiges Prüfverfahren sowie ein Verwaltungsstrafverfahren ein, in welchem die Videoanlage einer Handelsfiliale in Wien mit insgesamt 133 Kameras im Innen- und Außenbereich geprüft wurde.

Beanstandet wurden dabei u.a. Videokameras, die PIN-Eingaben von Kunden an Selbstbedienungskassen erfassten. Weiters wurden

[6] OGH 07.10.2025, 14 Os 95/25i

[7] BVwG 25. 7. 2025, GZ: W258 2299744-1/28E

diverse Kameras im Außenbereich beanstandet, die u.a. Gehsteig- und Straßenbereiche, einen Straßenbahn-Wartebereich, einen U-Bahn-Zugang und den Zugang zu einem Bahnhof erfassten.

Die DSB befand, dass das Unternehmen gegen die Grundsätze der Rechtmäßigkeit und Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a DSGVO) sowie gegen die rechtmäßige Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 DSGVO verstoßen hatte. Das Gebot der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO wurde außerdem durch fehlende „Privatzonenmaskierung" bzw. „Verpixeln" von datenschutzrechtlich relevanten Aufnahmebereichen der Videokameras verletzt.

Die DSB verhängte daher eine Geldbuße von EUR 1,5 Mio., woraufhin das beklagte Unternehmen Beschwerde beim BVwG erhob.

Im Juli 2025 gab das BVwG der Beschwerde teilweise Folge. Von den insgesamt neun durch die DSB beanstandeten Videokameras wurde für zwei Kameras das Straferkenntnis aufgehoben und das Strafverfahren eingestellt. Das BVwG stufte das Verhalten des Unternehmens jedoch in Summe als „grob fahrlässig" ein.

Unter Berücksichtigung der Schwere des Verstoßes, insb. der Anzahl der Betroffenen, der Dauer der Verstöße, der Erfassung der PIN-Codes von Kunden und der Aufnahme von „öffentlich zugänglichen hoch frequentierten" Bereichen ergab dies für das BVwG in Summe einen „Verstoß mit mittlerem Schweregrad". Die Höhe der verhängten Geldbuße von EUR 1,5 Mio. sah das BVwG aus „generalpräventiven Gründen" und unter Berücksichtigung der Konzernergebnisse 2024 als verhältnismäßig an und bestätigte sie.

Das Urteil des BVwG ist nicht rechtskräftig, da das Unternehmen Revision gegen die Entscheidung erhoben hat und dieser Fall nunmehr durch den VwGH zu entscheiden ist.

5. Bußgelder

Verstoß gegen die Rechte Betroffener bei der automatisierten Entscheidungsfindung: Bußgeld gegen deutsches Finanzunternehmen

In der durch den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit veröffentlichten Zwischenbilanz 2025 wird eine Entscheidung gegen ein nicht näher genanntes Finanzunternehmen in Deutschland mit einem Bußgeld in Höhe von EUR 492.000 angeführt.

Das Finanzunternehmen hatte zahlreiche Kreditkartenanträge mittels automatisierter Entscheidungen, d.h. Entscheidungen, die auf der Grundlage von Algorithmen und ohne menschliches Eingreifen getroffen wurden, abgelehnt, obwohl die Antragsteller über gute Bonität verfügten. Außerdem reagierte das Finanzunternehmen nicht angemessen auf Informationsanfragen und erfüllte daher die gesetzlich vorgeschriebenen Informations- und Auskunftspflichten nicht.

Automatisierte Entscheidungen, die maschinell auf algorithmischer Grundlage ohne menschliches Zutun getroffen werden, sind mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen verbunden. Der Einsatz solcher Verfahren ist nach Art. 22 DSGVO nur unter engen Voraussetzungen erlaubt. Neben höheren Anforderungen an die Rechtmäßigkeit haben die Verantwortlichen zusätzliche Informations- und Auskunftspflichten an Betroffene einzuhalten, die u.a. aussagekräftige Informationen über die involvierte Logik der automatisierten Entscheidung umfassen.

In derartigen Fällen kann das Bußgeld auch deutlich höher sein. Im konkreten Fall war das Unternehmen sehr bemüht, seinen Prozess zur Erfüllung von Rechten der betroffenen Personen bei einer automatisierten Entscheidungsfindung zu verbessern. Außerdem arbeitete es eng und umfassend mit dem Hamburgischen Beauftragten für Datenschutz und

Informationsfreiheit zusammen, was sich in diesem Fall strafmildernd auswirkte.

Fehlen der Rechtsgrundlage bei der Datenverarbeitung: Bußgeld gegen Experian

Die niederländische Datenschutzbehörde Autoriteit Persoonsgegevens verhängte gegen das Unternehmen Experian Nederland, einen Informationsdienstleister, eine Geldbuße in Höhe von EUR 2,7 Mio.

Zahlreiche Verbraucher, denen höhere Kautionen auferlegt oder die ganz abgelehnt wurden, wandten sich mit Beschwerden an die niederländische Datenschutzbehörde, worauf diese aktiv wurde. Bei diesen Fällen kam es im Hintergrund offensichtlich zu negativen Kreditauskünften für Betroffene, verursacht durch Experian.

Das Unternehmen hatte bis Anfang 2025 unrechtmäßig personenbezogene Daten von Betroffenen aus öffentlichen und privaten Quellen gesammelt, ohne Betroffene darüber ausreichend zu informieren. Diese gesammelten Daten wurden in weiterer Folge zur Erstellung von Kreditbewertungen für Kunden von Experian wie zB Telekommunikationsanbieter, Onlinehändler oder Vermieter verwendet.

Experian gestand im Verfahren den Verstoß gegen Art. 5 und Art. 6 DSGVO ein, beendete daraufhin seine Geschäftstätigkeit in den Niederlanden und löschte alle Daten.

Platzierung von Werbung und Setzen von Tracking-Cookies ohne (gültige) Einwilligung: EUR 325 Mio. Bußgeld gegen Google

Die französische Datenschutzbehörde verhängte ein erhebliches Bußgeld in Höhe von EUR 325 Mio. gegen Google LLC und Google Ireland Limited wegen Verstoß gegen Art. 82 des Französischen Datenschutzgesetzes.

Aufgrund der Beschwerde durch NOYB überprüfte CNIL die Website von Google und fand heraus, dass in den Postfächern des Google Mail-Dienstes (Gmail) Werbung so geschaltet wurde, dass sie den erhaltenen E-Mails sehr ähnelte. Darüber hinaus wurde dafür keine Einwilligung der Nutzer eingeholt. Zusätzlich wurden Nutzer bei der Kontoeinrichtung des Gmail-Dienstes dazu gedrängt, Tracker zu aktivieren, da es schwieriger war, die diesbezüglichen Cookies abzulehnen als anzunehmen.

Außerdem wurden die Nutzer nicht ausreichend über den Einsatz dieser Tracker informiert. Aus diesem Grund sah CNIL die Einwilligung als ungültig an.

Da dies bereits die dritte Bußgeldentscheidung von CNIL gegen Google im Zusammenhang mit dem Setzen von Cookies war, wurden diesmal noch weitere Auflagen erteilt, die Google binnen 6 Monaten zu erfüllen hat, anderenfalls eine Geldstrafe von EUR 100.000 pro Verzögerungstag droht.

Google hat nunmehr „Maßnahmen zu ergreifen, um die Anzeige von Werbung zwischen E-Mails in den Postfächern der Nutzer des Gmail-Dienstes ohne vorherige Zustimmung einzustellen und sicherzustellen, dass die Nutzer bei der Erstellung eines Google-Kontos ihre gültige Zustimmung zur Platzierung von Werbe-Cookies geben“.

Aus dieser Entscheidung geht einmal mehr deutlich hervor, dass Verantwortliche als Betreiber von Websites jedenfalls sicherzustellen haben, dass vor dem Schalten von Werbung oder Aktivieren von Trackern bzw. vor dem Setzen der Cookies die Einwilligung der Betroffenen einzuholen ist. Hierbei sind sog. Dark Patterns, d.h. manipulative Einwilligungsmechanismen, die Nutzer zu einem bestimmten Verhalten verleiten sollen, jedenfalls zu vermeiden.

Wichtig ist neben dem Einholen der Einwilligung in diesem Zusammenhang auch, dass die Nutzer von Websites immer klar, transparent, in geeigneter Form und umfassend informiert werden.

6. Rückblick auf den 14. Privacy Ring 2025 in Wien

Am 18. September 2025 fand im Hörsaal 1 der Universität Wien der 14. Privacy Ring statt. Unter dem Motto „Datenschutz in der digitalen Bedrohungslage“ wurden aktuelle Herausforderungen rund um Datenschutz und Privatsphäre in der digitalen Welt diskutiert.

Der hochkarätige Reigen an renommierten Sprecherinnen und Sprecher des Podiums aus dem DACH-Raum wurde durch Dr. Schmidl, dem Leiter der Österreichischen Datenschutzbehörde, komplettiert.

Das Podium gab abwechselnd spannende Einblicke in wirtschaftliche und gesellschaftliche Perspektiven aus den jeweiligen geografischen und fachlichen Bereichen.

Die nachfolgende Podiumsdiskussion bot für alle Teilnehmenden ausreichend Gelegenheit zum vertiefenden und lebhaften Austausch mit allerlei Fragen an das Podium.

Im Anschluss an die Veranstaltung konnten die Teilnehmenden den Nachmittag und frühen Abend bei einem Get-Together in lockerer Atmosphäre bei lokalen Köstlichkeiten ausklingen lassen. Dabei wurden in ungezwungenem Rahmen nicht nur neue Kontakte geknüpft, sondern auch Erkenntnisse und Erfahrungen aus der internationalen Praxis ausgetauscht, was die Veranstaltung insgesamt zu einem großen Erfolg machte.

••••

Save the Date – Datenschutzseminar

Es freut uns, Ihnen unser nächstes jährliches Datenschutz-Praxisseminar am **24. und 25. März 2026** im Hilton Vienna Plaza anzukündigen. In unserem bewährten Seminar vermitteln wir Ihnen 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.

Save the Date – Privacy Ring 2026 in Liechtenstein

Der **15. Privacy Ring** des Datenschutzverein Privacy Ring findet 12. Februar 2026 in Liechtenstein statt. Nähere Informationen dazu finden Sie in Kürze auf der Secur-Data Website und in der nächsten Ausgabe des DSG-Info-Service!