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 2026 Ausgabe Nr. 121

Liebe Leserinnen und Leser,

das Datenschutzjahr 2026 verspricht wieder spannend zu werden. Die Fahrtrichtung des „Digitalen Omnibus" ist noch nicht klar erkennbar, den aktuellen Stand zu Redaktionsschluss erläutern wir Ihnen hier kurz.

In dieser Ausgabe geben wir Ihnen wieder einen kompakten Überblick über aktuelle, rechtliche Entwicklungen: dieses Mal zur neuen Verordnung 2518/2025, zu Empfehlungen des Europäischen Datenschutzausschusses EDSA für Betreiber von E-Commerce Websites, Aktuelles zu einem neuen Angemessenheitsbeschluss der EU-Kommission sowie Neuigkeiten aus der nationalen und internationalen Judikatur. Auch zeigen wir dabei die Bedeutung für die betriebliche Praxis sowie konkrete Handlungsoptionen auf.

Der im Februar 2026 in Liechtenstein stattgefundene Privacy Ring war von großem Erfolg gekrönt und erhielt sehr viel positiven Zuspruch durch die überdurchschnittlich hohe Teilnehmerzahl in diesem Jahr.

Besonders hervorheben möchten wir unser jährliches und in diesem Jahr nur einmalig stattfindendes Praxisseminar am 24. und 25. März 2026. Dabei bieten wir Ihnen insbesondere die Möglichkeit zum vertiefenden Dialog und fachlichen Austausch. Wir freuen uns schon sehr, alle Teilnehmenden bei unserem Seminar persönlich begrüßen zu dürfen!

Wir wünschen eine angenehme Lektüre!

Mag. Judith Leschanz
Geschäftsführung

1. Neue Verfahrensregeln durch Verordnung (EU) 2025/2518

Allgemeines zur Verordnung (EU) 2025/2518

Per 12. Dezember 2025 wurde im Amtsblatt der EU die **Verordnung (EU) 2025/2518**[1] **zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der EU-Datenschutz Grundverordnung (DSGVO)** veröffentlicht.

Diese Verordnung trat mit 1. Jänner 2026 in Kraft und sind die Bestimmungen ab 2. April 2027 anwendbar.

Mit dieser neuen Verordnung wird ein bedeutender Schritt zur **Vereinheitlichung der Durchsetzung der DSGVO** gesetzt. Die materiell-rechtlichen Pflichten aus der DSGVO bleiben durch die Verordnung jedenfalls unverändert.

[1] https://eur-lex.europa.eu/eli/reg/2025/2518/oj

Es werden darin **Rahmenbedingungen für grenzüberschreitende Ermittlungs- und Beschwerdeverfahren** und die diesbezügliche **Datenverarbeitung** neu geordnet. Durch die neuen Vorschriften werden insbesondere strengere Fristen, vereinheitlichte Anforderungen an Beschwerden sowie gestärkte Verteidigungsrechte für betroffene Organisationen eingeführt.

Bisher gab es bei grenzüberschreitenden DSGVO-Verfahren durch den sog. „One-Stop-Shop"-Mechanismus der Aufsichtsbehörden, wonach bei grenzüberschreitenden Sachverhalten eine federführende Aufsichtsbehörde zuständig ist, regelmäßige massive Zeitverzögerungen und Rechtsunsicherheiten in den Verfahren und dadurch mangelnde Effizienz.

Konkrete Änderungen

Die Verordnung enthält insb. die folgenden verfahrensrechtlichen Bestimmungen:

- Harmonisierte Voraussetzungen für Beschwerden nach der DSGVO

Die aktuell oft sehr variierenden Anforderungen der nationalen Aufsichtsbehörden bei Beschwerdeverfahren werden nunmehr vereinheitlicht. Die Verordnung enthält dazu eine taxative Liste von Zulässigkeitsvoraussetzungen für Beschwerden und dürfen darüber hinaus keine weiteren Informationen gefordert werden.

- Stärkung der prozessualen Rechte von Beschwerdeführern und Verantwortlichen bzw. Auftragsverarbeitern als untersuchte Parteien

Hierbei erhalten alle untersuchten Parteien ein „Recht auf Gehör" sowie Informationen im Zuge der Mitteilung vorläufiger Feststellungen. Ergänzend dazu wird allen Beteiligten im Verfahren umfassende Akteneinsicht gewährt.

- Einführung verbindlicher Deadlines für die Verfahrensdauer

Künftig sollen alle Standard-Verfahren maximal 15 Monate dauern, wobei es eingeschränkt eine Verlängerungsmöglichkeit von 12 Monaten bei komplexeren Fällen gibt. Außerdem wird die Möglichkeit einer frühzeitigen Streitbeilegung explizit geregelt.

- Klarere Zusammenarbeit zwischen den Aufsichtsbehörden

Im Zuge von sowohl vereinfachten wie auch komplexeren Verfahren haben die federführenden Aufsichtsbehörden die Pflicht, mit den anderen betroffenen Datenschutzbehörden zusammenzuarbeiten.

Die Kooperation zwischen den einzelnen Aufsichtsbehörden soll durch die neuen Verfahrensvorschriften vereinheitlicht und der Informationsaustausch klar dargestellt werden, einschließlich eines Eskalationsprozesses an den Europäischen Datenschutzausschuss.

Auswirkungen

Wichtig ist, dass diese Verordnung weder die Grundlagen der DSGVO noch nationale Datenschutzvorschriften ändert oder ersetzt. Es sollen durch die neuen Regelungen ausschließlich **zentrale, prozessuale Vorschriften vereinfacht** werden.

Durch die Einführung **verbindlicher Zeitlimits** wird es zu einer **Beschleunigung der Verfahren** kommen und sollen nunmehr unbefristete „Endlos"-Verfahren der Vergangenheit angehören.

Zusammengefasst bringt die Harmonisierung der Vorschriften in der neuen Verordnung für alle Beteiligten deutliche Vorteile durch mehr **Rechtssicherheit in der grenzüberschreitenden Beschwerdedurchsetzung**.

Datenschutz-Seminar 2026

Die Entwicklung des nationalen und internationalen Datenschutzes geht weiter, auch 2026 sind neue rechtliche Entscheidungen und Aktualisierungen zu erwarten. Lassen Sie sich im bewährt kleinen Kreis von unseren Top-Expertinnen und -Experten über alle wesentlichen Neuerungen in Angelegenheiten der Informationssicherheit und der Datenschutzpraxis informieren und erhalten Sie dabei einen kompakten und zugleich fundierten Überblick über aktuelle gesetzliche Entwicklungen sowie praxisrelevante Rechtsprechung!

Neben praxisnaher Wissensvermittlung steht Secur-Data für State-of-the-Art-Anwendungstipps sowie praxistaugliche Muster und Vorlagen. Auch heuer wird Ihnen wieder **ein Vertreter der österreichischen Datenschutzbehörde** aktuelle Judikatur der DSB präsentieren und auf Ihre Fragen eingehen.

24. März 2026, 9:15 – 17:00 Uhr:

„Rechtliche Themen und Entwicklungen (Modul 1)“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Mag. Gertraud Wisiak, Mag. Rona Paca
Gastreferent: Vertreter der Österreichischen Datenschutzbehörde

25. März 2026, 9:15 – 17:00 Uhr:

„Praktische Umsetzung (Modul 2)“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Mag. Gertraud Wisiak, Mag. Rona Paca, Mag. Krzysztof Müller

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.

2. Rückblick auf den 15. Privacy Ring 2026 in Liechtenstein

Der **15.** Privacy Ring fand am 12. Februar 2026 in den Räumlichkeiten der Universität Liechtenstein in Vaduz statt.

Als internationale Fachtagung im gesamten DACHLI-Raum greift der Privacy Ring stets aktuelle Entwicklungen auf und richtet den **Fokus auf die datenschutzrechtlichen Fragestellungen** unserer Zeit.

Das zentrale Motto in diesem Jahr war **„Datenschutz und neue Technologien – zwischen Regulierung und Praxis“**.

Dabei stand das Thema der **Künstlichen Intelligenz** – als Teil unseres täglichen Alltags – und dessen **Bedeutung für die Datenschutz-Praxis im Fokus**. Die spannenden und informativen Fachvorträge hochkarätiger DatenschutzexpertInnen behandelten Themen wie IT-Sicherheit mit Datenschutz, Cloud-Dienste und Datentransfer, aktuelle Herausforderungen der Aufsichtsbehörden zur Informationsfreiheit, bis hin zu Berichten zur aktuellen Judikatur im Datenschutzbereich. Zum Abschluss fand eine

lebhafte Podiumsdiskussion zum Thema Microsoft 365 statt.

Die außerordentlich **hohe Teilnehmerzahl des diesjährigen Privacy Ring** und die zahlreichen positiven Rückmeldungen auf die Veranstaltungen zeigen eindrucksvoll den **Erfolg dieser Tagung** und unterstreichen die Bedeutung derart internationaler Veranstaltungen für DatenschutzexpertInnen.

3. Empfehlungen des Europäischen Datenschutzausschusses zur Erstellung von Nutzerkonten auf E-Commerce-Websites

Wir möchten Sie auf eine vor kurzem veröffentlichte Empfehlung des Europäischen Datenschutzausschusses (ESDA) mit dem Titel „**Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites“** zum Thema der Rechtsgrundlage für die Verpflichtung zur Erstellung von Nutzerkonten auf E-Commerce-Websites[2] hinweisen. Die diesbezügliche Konsultation endete Mitte Februar 2026.

Darin befasst sich der EDSA im Speziellen mit der Frage der häufig **verpflichtenden Erstellung eines Online-Kontos für Nutzer von E-Commerce-Websites,** nach der erst Angebote bzw. Waren und Dienstleistungen erworben werden können. Das Dokument enthält **Empfehlungen für Verantwortliche im E-Commerce-Sektor**, wann diese die Erstellung eines Kontos nach Art. 5 Abs. 1 lit. a und Art. 6 DSGVO verpflichtend verlangen dürfen. Insbesondere werden **konkrete Fälle für die Rechtmäßigkeit** der Erstellung eines Nutzerkontos und Datenverarbeitung durch Verantwortliche zur Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO), Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO) oder Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) genannt.

Schließlich hält der EDSA fest, dass die **verpflichtende Erstellung eines Nutzerkontos nur in wenigen Fällen** (zB beim Angebot eines Abonnementdienstes oder bei der Bereitstellung exklusiver Angebote) dem jeweiligen Verarbeitungsweck entspricht und damit **rechtmäßig** ist.

Daher kommt der EDSA zum Ergebnis, dass es für eine rechtmäßige Datenverarbeitung effizienter ist, wenn Verantwortliche **Nutzern** auf E-Commerce-Websites **die Wahl lassen**, entweder ein **Konto zu eröffnen oder als Gast einzukaufen**. Beim einem solchen „Gast“-Modus werden laut EDSA insb. auch die Grundsätze **„Privacy by Design“ und „Privacy by Default“ gemäß Art. 25 DSGVO** bestmöglich erfüllt.

4. Neuer Angemessenheitsbeschluss der Kommission mit Brasilien

Wie schon im DSG Info Service 120 mitgeteilt, führte die Europäische Kommission (EK) bereits seit 2023 Verhandlungen mit Brasilien zum Abschluss eines Angemessenheitsbeschlusses gemäß Art. 45 DSGVO (bzw. gemäß Art. 36 der RL (EU) 2016/680[3]).

Im Zuge der nunmehr abgeschlossenen **Verhandlungen zum Freihandelsabkommen Mercosur** konnte auch bzgl. des Angemessenheitsbeschlusses mit Brasilien ein Abschluss erzielt werden. Am 17. Jänner 2026 kam es zum Abschluss[4] eines **Partnerschaftsab-**

[2] https://kurzlinks.de/cqoi
[3] https://kurzlinks.de/l2qu
[4] https://kurzlinks.de/lfsm

kommens (EMPA) und des vorläufigen Handelsabkommens (Interims Trade Agreement) zwischen EU und Mercosur.

Diese zwischen den EU-Staaten und den **Mercosur-Staaten Argentinien, Brasilien, Paraguay und Uruguay** abgeschlossenen Abkommen bedeuten zahlreiche **Handelserleichterungen** und damit wirtschaftliche und strategische Vorteile für europäische Unternehmen.

Der **Angemessenheitsbeschluss**[5] **mit Brasilien** basiert darauf, dass Brasilien 2018 ein Datenschutzgesetz nach Vorbild der DSGVO verabschiedet und seither eine unabhängige Behörde geschaffen hat.

Somit ist nunmehr gewährleistet, dass Brasilien ein **angemessenes Schutzniveau** für die **Verarbeitung personenbezogener Daten** bietet und daher personenbezogene Daten **ohne zusätzliche Schutzmaßnahmen** zwischen der EU und Brasilien übermittelt werden können. Die Europäische Kommission hat zusätzlich angekündigt, das Funktionieren des Angemessenheitsbeschlusses nach vier Jahren zu überprüfen.

5. Aktuelles zum Digitalen Omnibus

Wie im DSG Info Service Nr. 120 ausführlich berichtet, liegen seit November 2025 Pläne für den sog**. „Digitalen Omnibus" in zwei Teilen** – im ersten Teil[6] Änderungen zum Data Act und der DSGVO, im zweiten Teil[7] Änderungen zum AI Act[8] – vor.

Alle Änderungsvorschläge als Teil des Omnibus-Gesamtpakets[9] der EU sollen zu **Bürokratieabbau** und **Stärkung und Wachstum der Wettbewerbsfähigkeit** in der EU beitragen bzw. diese fördern.

Die aktuellen Legislativvorschläge zum Digitalen Omnibus wurden dem **EU-Parlament und dem Rat bereits Ende 2025** zur Prüfung und Annahme vorgelegt. Mitte Jänner 2026 wurde der Europaabgeordnete **Michael McNamara** zum **Berichterstatter für das „AI Omnibus"-Paket** (Änderungen zum AI Act) ernannt.

Die aktuelle Ratspräsidentschaft Zypern plant, bis Ende Juni 2026 zumindest die ratsinternen Verhandlungen abzuschließen. Aufgrund der zahlreichen und weitreichenden Änderungen kann es jedoch einige Monate oder vielleicht sogar Jahre dauern, bis alle Regelungen beschlossen sind und in Kraft treten.

In einer **Aussendung**[10] vom 11. Februar 2026 äußerte sich der **Europäische Datenschutzausschuss** (EDSA) gemeinsam mit dem **Europäischen Datenschutzbeauftragten** (EDSB) zu den Entwürfen des Digitalen Omnibus.

Beide Institutionen **unterstützen** darin die **geplanten Vereinfachungen** und die sich daraus ergebende Stärkung der Wettbewerbsfähigkeit für EU-Unternehmen. Jedoch sollten die **Änderungen** durch den Digitalen Omnibus **„nicht zulasten der Grundrechte"** erfolgen.

Weiters werden die **Vereinfachung der Informationsanforderungen** und die **Verringerung des Verwaltungsaufwands** von beiden Institutionen begrüßt, jedoch sollten zusätzliche Klarstellungen zur Sicherstellung von Rechtssicherheit getroffen werden.

Sowohl EDSA als auch EDSB äußern gleichzeitig **Bedenken zu Änderungen** insb. der DSGVO.

Beide fordern dazu auf, die vorgeschlagenen Änderungen insb. zur **Definition personenbezogener Daten** im Gesetzgebungsprozess in der vorgeschlagenen Version nicht anzunehmen, da diese weit über eine **gezielte oder**

[5] https://kurzlinks.de/92eg
[6] https://kurzlinks.de/y1xu
[7] https://kurzlinks.de/ict0
[8] https://kurzlinks.de/oflw
[9] https://kurzlinks.de/s25m
[10] https://kurzlinks.de/n3ei

technische Änderung der DSGVO hinausgehen.

Bereits am 20. Jänner 2026 haben EDSA und EDSB auf Ersuchen der Kommission eine gemeinsame **Stellungnahme**[11] zum **Digitalen Omnibus bzgl. des AI Act** abgegeben. Auch darin äußern sie sich positiv zu Vereinfachungen des AI Act, jedoch haben beide Institutionen **Bedenken** dahingehend, dass die Änderungen nicht den **Schutz der Grundrechte** des Einzelnen und auch nicht die **Unabhängigkeit und Aufgaben der Datenschutzbehörden einschränken** dürfen.

Ende Februar 2026 wurde nunmehr ein **geänderter Entwurf zum Digitalen Omnibus** bzgl. DSGVO u.a. von Euractiv **geleakt.**[12] Nach Widerständen einiger EU-Mitgliedsstaaten, darunter Österreich, soll nunmehr die geplante **Ergänzung der Definition personenbezogener Daten in Art. 4 Z 1 DSGVO gestrichen** werden. Dabei geht es um die Ausnahme, dass Daten dann nicht als personenbezogen gelten, wenn Unternehmen nicht in der Lage sind, diese zu identifizieren. Diese Änderungen sollen laut Medieninformationen nunmehr dem Ausschuss der Ständigen Vertreter im Rat vorgelegt werden.[13]

Aufgrund der **Uneinigkeit innerhalb der EU-Mitgliedsstaaten** und der sehr **kritischen Worte von EDSA und EDSB zum Digitalen Omnibus** bleibt abzuwarten, wie es jetzt konkret weitergeht und auch in welchem Tempo. Als nächstes werden die Stellungnahmen des Rates und des Europäischen Parlaments zum Digitalen Omnibus bzgl. DSGVO und AI Act erwartet.

Wir werden Sie darüber jedenfalls auf dem Laufenden halten.

6. Neues aus der Rechtsprechung

Urteil des Thüringer Oberlandesgerichts zu Gesichtserkennungssoftware bei Prüfungen und immateriellem Schadenersatz

Das Thüringer Oberlandesgericht hat sich in einem Urteil[14] vom 13. Oktober 2025 (Az.: 3 U 885/24) mit der Frage der **Verarbeitung von biometrischen Daten durch eine Gesichtserkennungssoftware bei Fernprüfungen** befasst.

Ausgangspunkt war die Klage einer Studentin der Universität Erfurt. Während der COVID-Pandemie hatte die Universität bei elektronischen Fernprüfungen Gesichtserkennungssoftware eingesetzt, um **Täuschungsversuche** bei Fernprüfungen bestmöglich **zu verhindern**.

Dabei wurden während der Prüfung in unregelmäßigen Abständen die **von den Webcams** der Studierenden **aufgenommenen Bilder** mit vorliegenden Bildern der betroffenen Personen verglichen. Bei mangelnder Übereinstimmung gab das System eine Meldung ab. Dieses Verfahren zur digitalen Prüfungsaufsicht wird auch **„Proctoring“** genannt.

Die Studentin klagte die Universität, da sie sich während der Prüfung „unter erheblichen Stress gesetzt“ fühlte, und verlangte **Schadenersatz** iHv EUR 1.000.

Das OLG Thüringen stellte fest, dass die Studentin **keine wirksame (ausdrückliche) Einwilligung nach Art. 9 DSGVO** erteilt hatte und somit die **Verarbeitung** durch die Gesichtserkennungssoftware **rechtswidrig** war.

Den **Anspruch auf immateriellen Schadenersatz** erkannte das OLG zwar an, aber nur zu 20 Prozent, und sprach der Studentin EUR 200 an Schadenersatz zu. Das Gericht sah zwar in diesem Fall **keinen Kontrollverlust der Daten**, da die Klägerin schon seit Jahren ihr Gesicht auf diversen Plattformen, zB Instagram, veröffent-

[11] https://kurzlinks.de/lymx
[12] https://kurzlinks.de/9pu3
[13] https://kurzlinks.de/dp9m
[14] https://kurzlinks.de/5d68

lich hatte. Es stellte jedoch eine **Beeinträchtigung** der Klägerin mit dem Gefühl, **„der Technik ausgeliefert zu sein“** fest und sprach daher einen (geringen) immateriellen Schadenersatz zu.

Diese Entscheidung zeigt, dass **jede technische Neuentwicklung** – vor allem iZm **KI** – , sei sie auch noch so bedeutend oder, wie im Urteil beschrieben, während der COVID-Pandemie von „gewissem öffentlichen Interesse“, immer auch unter **Berücksichtigung datenschutzrechtlicher Aspekte** genau zu prüfen ist. Dabei kann auch, insb. wenn es um biometrische Daten geht, die persönliche Betroffenheit bzw. Belastung jedes Einzelnen unterschiedlich ausfallen.

Erneute Entscheidung der Österreichischen Datenschutzbehörde (DSB) zum Einsatz von Microsoft 365 Education

Bezugnehmend auf unsere Information im DSG Info Service 119 über die Entscheidung der DSB[15] im Oktober 2025 gibt es nunmehr eine weitere Entscheidung[16] gegen Microsoft in Zusammenhang mit dem **Einsatz von Cookies bei Microsoft 365 Education an österreichischen Schulen.**

Auch im aktuellen Fall wurde die DSB aufgrund einer Beschwerde von NOYB[17] tätig.

Im konkreten Fall stellte die DSB erneut einen **Verstoß gegen das Recht auf Auskunft** nach Art. 15 DSGVO fest. In diesem Fall ging es darüber hinaus um die detaillierte Prüfung der durch Microsoft gesetzten Tracking Cookies.

Hierbei stellte die DSB die **Rechtwidrigkeit** der Verarbeitung durch das **Setzen von Tracking Cookies** dahingehend fest, dass Cookies „mit einzigartigen, zufallsgenerierten Werten“ am jeweiligen Endgerät gesetzt wurden und die **„technische Erforderlichkeit“ der Cookies nicht gegeben** war. Es wurden das **Nutzungsverhalten** durch die gesetzten Cookies **analysiert**, Browserdaten gesammelt und diese **Daten für Werbung** verwendet. Da von der Microsoft Corporation als Verantwortlichem nach Art. 4 Z 7 DSGVO **keine Einwilligung eingeholt** wurde, war die **Verarbeitung** ohne Vorliegen eines Erlaubnistatbestands **nach Art. 6 Abs. 1 DSGVO rechtswidrig**.

Schließlich hielt die DSB auch fest, dass sofern die **Datenverarbeitung** Im Zuge der Bereitstellung von Microsoft 365 Education „ausschließlich zu schulischen Zwecken erfolgt“, nicht die gesamte Datenverarbeitung, sondern nur der **Einsatz der Tracking Cookies unrechtmäßig** ist.

In Deutschland ist die Situation rund um den Einsatz von Microsoft 365 deutlich angespannter. So stellte **die Deutsche Datenschutzkonferenz**[18] bereits 2022 fest, dass bzgl. **Microsoft-Anwendungen,** insbesondere im Zusammenhang mit dem **Drittlandsdatentransfer** und der **mangelnden Transparenz,** ein Nachweis des **datenschutzrechtskonformen Einsatzes nicht gegeben** ist. Auch die aktuelle Diskussion[19] um den Freistaat Bayern, welcher plant, einen Vertrag über die Nutzung des Cloud-Office-Pakets von Microsoft 365 in Höhe von ca. EUR 1 Mrd. für die gesamte bayerische Verwaltung abzuschließen, zeigt die **Umstrittenheit des Einsatzes** rund um Microsoft-Systeme.

[15] DSB 08.10.2025, GZ: D135.027 2025-0.477.534
[16] DSB 21.01.2026, GZ: D135.026 2025-0.768.263
[17] https://kurzlinks.de/2n8p
[18] https://kurzlinks.de/6mhv
[19] https://kurzlinks.de/1h8d

Beratung im Bereich Künstliche Intelligenz: KI-Strategie

Aktuelle Studien zeigen es deutlich:

- 4 von 10 Unternehmen scheitern an KI-Strategie
- Jedes 2. 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!

7. Verwaltungsstrafen

Verstöße gegen Sicherheit der Verarbeitung: Hohe Strafen durch die französische Datenschutzbehörde – Fall 1

Die **französische Datenschutzbehörde CNIL** verhängte hohe **Geldstrafen gegen** die Unternehmen **FREE und FREE MOBILE**, zwei Telekommunikationsdienstleister-Töchter des ILIAD-Telekomkonzerns.

Ausgangspunkt war ein **externer Angriff** auf die Informationssysteme beider Telekomdienstleister, durch die Angreifer diverse **Daten von über 24 Mio. Kunden** beider Unternehmen, inklusive Bankdaten, erhalten haben.

Aufgrund einer Vielzahl von Beschwerden an die CNIL prüfte die Datenschutzbehörde beide Unternehmer im Zusammenhang mit dem Datenleck. Dabei stellte CNIL **erhebliche Sicherheitsmängel bei beiden Telekomdienstleistern**, speziell **Versäumnisse bei** der Implementierung **technischer und organisatorischer Maßnahmen** und damit Gewährleistung der **Sicherheit personenbezogener Daten** nach Art. 32 DSGVO, fest. Im Besonderen war das VPN-Authentifizierungsverfahren technisch nicht ausreichend robust.

Außerdem versäumten es die Telekomdienstleister, mit den **betroffenen Person** nach dem Datenschutzverstoß ausreichend **zu kommunizieren** (Art. 34 DSGVO). Die in zwei Stufen erfolgten Meldungen an Betroffene enthielten zu wenig Informationen, um den genauen Umfang des Vorfalls und die Folgen für alle Betroffenen verstehen zu können.

Bei FREE MOBILE wurden darüber hinaus auch Versäumnisse bei der Sortierung von Daten, insbesondere Schwierigkeiten bei der **Einhaltung von Aufbewahrungs- sowie Löschfristen**, und daher Verstöße gegen Art. 5 DSGVO festgestellt.

Sowohl FREE als auch FREE MOBILE waren jeweils für die Verarbeitung der Daten ihrer eigenen Abonnenten Verantwortliche nach Art. 4 Z 7 DSGVO. Daher verhängte **CNIL gegen beide Unternehmen** jeweils eine **Strafe**, EUR 27 Mio. gegen FREE MOBILE und EUR 15 Mio. gegen FREE, in **Summe EUR 42 Mio**.

Als Begründung für die hohen Strafen führte CNIL insb. die **mangelnde Kenntnis wesentlicher Sicherheitsprinzipien**, die **hohe Zahl der Betroffenen** und die speziell durch den **Verlust der Bankdaten** entstandenen sehr hohen Risiken an.

Bei diesem gleich zwei Telekomdienstleister betreffenden Verfahren zeigt sich, wie wichtig und aktuell die **Implementierung geeigneter Sicherheitsmaßnahmen** zum Schutz von personenbezogenen Daten von Kunden ist. Die **Folgen** fehlender Sicherheitsmaßnahmen können dabei äußerst **geschäftskritisch und auch geschäftsschädigend** sein.

Verstöße gegen Sicherheit der Verarbeitung: Hohe Strafen durch die französische Datenschutzbehörde – Fall 2

In einem weiteren Fall sprach die **französiche Datenschutzbehörde CNIL** erneut eine Geldstrafe in Höhe von EUR 5 Mio. aufgrund des Verstoßes gegen die Sicherheit der Verarbeitung aus.

Hintergrund der Entscheidung der CNIL war das Unternehmen **France Travail**, die französische Arbeitsagentur, welches Opfer eines Angriffs durch **Social Engineering** wurde. Durch diesen Angriff wurden **Daten** von **über 40 Mio**. arbeitsuchenden **Personen gestohlen**. Konkret wurden die Konten von Beratern der Arbeitsagentur von Externen „übernommen“ und dadurch Kontakt- und Adressdaten sowie Daten zur Sozialversicherung erbeutet, u.a. von Personen, die sich bereits vor 20 Jahren registriert hatten.

Auch bei France Travail stellte die CNIL gravierende **Mängel bei den implementierten technischen und organisatorischen Maß-**

nahmen und somit der **Sicherheit der Verarbeitung von Daten** nach Art. 32 DSGVO fest. Einerseits waren **die Authentifizierungsmechanismen** der Arbeitsagentur **zu schwach** und wurden andererseits **keine technischen Maßnahmen gesetzt**, um derartige externe Angriffe zu erschweren bzw. zu verhindern.

Zusätzlich gab es in der Arbeitsagentur **unzureichende Berechtigungskonzepte**, mangelhafte **Passwortrichtlinien** und offenbar einen **Mangel an Wissen**, wie solche Fälle zu vermeiden sind.

Die französische Datenschutzbehörde verhängte gegen die Arbeitsagentur eine **Strafe** in Höhe von **EUR 5 Mio**. und zugleich die **Auflage der sofortigen Behebung**, ansonsten würden pro Tag EUR 5.000 zusätzlich verhängt.

Dieser Fall zeigt deutlich, wie verheerend die **Folgen von Social Engineering-Attacken** sein können und welche massiven **Auswirkungen mangelhafte Sicherheitsvorkehrungen** auf den Betrieb und die Daten von Kunden haben können, sowohl **finanziell** und **reputationsmäßig** als auch **geschäftspolitisch**.

Daher ist es immens wichtig, **wirksame technischen und organisatorische Maßnahmen** nach dem Stand der Technik einzusetzen, und vor allem **regelmäßige Schulungen** der Mitarbeitenden zur Sensibilisierung für Gefahren, insb. durch Social Engineering und Vermeidung derartiger Attacken, durchzuführen.

••••