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

Oktober 2024 Ausgabe Nr. 115

Liebe Leserinnen und Leser,

in dieser Ausgabe unserer DSG-Info erwarten Sie spannende Einblicke in die neuesten Entwicklungen im Datenschutzrecht. Wir beleuchten die Pflichten rund um den Digital Operational Resilience Act, der ab Jänner 2025 in Österreich wirksam wird und berichten über teure Datenschutzvergehen von internationalen Konzernen, aber auch KMUs. Wir präsentieren Ihnen auch wie gewohnt aktuelle Rechtsprechung und Updates aus der EU.

Im November informieren wir Sie im Rahmen unseres Datenschutzpraxisseminars über aktuelle Entwicklungen und Best Practices. Nähere Infos finden Sie hier und in unserer DSG-Info.

Wir wünschen eine angenehme Lektüre!

Mag. Judith Leschanz
Geschäftsführung

1. Finanzmarktaufsicht in Österreich mahnt: Rechtzeitig auf DORA vorbereiten!

Vor wenigen Wochen hat ein fehlerhaftes Update der CrowdStrike-Software eine weltweite Krise ausgelöst und verdeutlicht, dass nicht nur Cyberangriffe, sondern auch Produktmängel gravierende IT-Risiken darstellen können.

Um solche Risiken zu behandeln, wird die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, kurz DORA)[1] ab dem 17. Jänner 2025 in Österreich wirksam. DORA hat das Ziel, die Widerstandsfähigkeit europäischer Finanzunternehmen gegenüber Cyber-Risiken und IT-bedingten Betriebsstörungen zu stärken und rückt die Informations- und Kommunikationstechnologien (IKT) in den regulatorischen Fokus.

Zudem werden erstmals auch als kritisch eingestufte IKT-Drittanbieter in den Überwachungsrahmen einbezogen.

Laut FMA müssen betroffene Finanzdienstleister und Drittanbieter sich in den kommenden Wochen und Monaten auf das neue Aufsichtsregime vorbereiten, da DORA ohne Übergangsfristen vollumfänglich gilt.

Um die Umsetzung von DORA zu erleichtern, hat die FMA einen speziellen DORA-Bereich[2] auf ihrer Website eingerichtet, der die relevanten Regularien und Anforderungen zusammenfasst. Dort werden die technischen Regulierungs- und Durchführungsstandards detailliert

[1] **https://kurzlinks.de/5kio**

[2] **https://kurzlinks.de/1i50**

erläutert und häufig gestellte Fragen in einem umfassenden Q&A-Format beantwortet. Hilfreiche Informationen finden Sie auch auf der Website der BaFin[3].

Das DORA-Regulierungspaket soll bestehende Gesetzgebungslücken für Finanzdienstleister schließen und konsolidiert somit das zuvor verstreute Regelwerk. Es beinhaltet umfassende Berichts-, Informations- und Überwachungspflichten. Betroffene Unternehmen müssen unter anderem

- einen IKT-Risikomanagementrahmen und Business Continuity Management implementieren;
- zahlreiche Berichtspflichten erfüllen, insbesondere zu Verträgen mit IKT-Drittanbietern und IKT-Vorfällen;
- die digitale Betriebsstabilität regelmäßig testen, auch durch zentrale, bedrohungsorientierte Penetrationstests;
- Risiken von IKT-Drittanbietern steuern und überwachen;
- regelmäßigen Informationsaustausch zwischen den betroffenen Unternehmen institutionalisieren.

Ab der verpflichtenden Anwendung von DORA müssen alle bestehenden Verträge mit IKT-Drittanbietern den neuen Anforderungen entsprechen. Unternehmen in Österreich sind verpflichtet, der FMA umgehend ein Informationsregister zu allen Verträgen mit IKT-Drittdienstleistern zu übermitteln. Zudem müssen schwerwiegende Cyber-Vorfälle und IKT-bedingte Betriebsstörungen innerhalb der festgelegten Fristen gemeldet werden:

Erstmeldung: Muss so schnell wie möglich erfolgen, spätestens innerhalb von 4 Stunden nach Einstufung als schwerwiegender Vorfall und spätestens 24 Stunden nach Entdeckung (Art. 6 Abs. 1a Draft RTS)[4].

Zwischenmeldung: Muss innerhalb von 72 Stunden nach der Erstmeldung oder nach Wiederherstellung des regulären Geschäftsbetriebs übermittelt werden, oder sobald sich der Vorfallstatus oder die Handhabung des Vorfalls wesentlich ändert. Zusätzliche Aktualisierungen müssen erfolgen, wenn neue Informationen verfügbar sind oder auf Antrag der Behörde (Art. 6 Abs. 1b Draft RTS, Art. 19 Abs. 4 DORA-VO).

Abschlussmeldung: Muss spätestens einen Monat nach der letzten Zwischenmeldung übermittelt werden (Art. 6 Abs. 1c Draft RTS).

Unternehmen, die bereits Erfahrungen mit der Umsetzung der DSGVO gesammelt haben, können dieses Wissen nun für DORA nutzen, um die Einhaltung der Vorschriften sicherzustellen. Die Hauptaufgaben sind dabei ähnlich: Daten vollständig analysieren, Verträge überprüfen, Sicherheit sicherstellen und Mitarbeiter schulen. Wer bereits entsprechende Strukturen und Abläufe eingeführt hat, spart Zeit und Mühe.

2. 91 Millionen Euro Bußgeld für Meta

Die irische Datenschutzbehörde (DPC) hat Meta erneut mit einer Strafe belegt – diesmal in Höhe von 91 Millionen Euro. Grund dafür war ein Sicherheitsvorfall im Jahr 2019, bei dem Meta ca. hundert Millionen Passwörter unverschlüsselt auf seinen Servern speicherte.

Die DPC begann im April 2019 mit der Untersuchung, nachdem Meta den Vorfall gemeldet hatte. Dabei stellte sich heraus, dass Meta aufgrund unzulänglicher Sicherheitsmaßnahmen gegen die DSGVO verstoßen hatte. Das Risiko war erheblich, da unbefugte Dritte dadurch auf

[3] **https://kurzlinks.de/bb3r**

[4] siehe **https://kurzlinks.de/olra**

Social-Media-Konten und möglicherweise auch auf sensible Informationen zugreifen konnten. Zusätzlich meldete Meta den Vorfall nicht innerhalb der vorgeschriebenen 72 Stunden und dokumentierte ihn nicht korrekt.

Graham Doyle, der stellvertretende Kommissar der DPC, betonte, dass es allgemein als Standard gilt, Passwörter niemals unverschlüsselt oder im Klartext zu speichern, da dies mit hohem Missbrauchsrisiko verbunden ist.

Meta erklärte, dass der Fehler in den Passwortmanagement-Prozessen nach einer internen Überprüfung im Jahr 2019 entdeckt und umgehend behoben wurde. Es gebe keine Hinweise darauf, dass die Passwörter missbraucht oder unbefugt abgerufen wurden.

Die Geldstrafe ist höher als ein früheres Bußgeld von 17 Mio. EUR, das Meta 2022 für einen Vorfall erhielt, bei dem bis zu 30 Mio. Nutzer betroffen waren. Dies spiegelt eine Tendenz zu höheren Bußgeldern wider, die sich zunehmend durchsetzt und darauf abzielt, Unternehmen stärker für den Schutz von Nutzerdaten zur Verantwortung zu ziehen.

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 bewährt 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 **eine Vertreterin der österreichischen Datenschutzbehörde** die aktuelle Judikatur der DSB präsentieren und auf Ihre Fragen eingehen.

11. November 2024, 9:15 – 17:00 Uhr:

„Rechtsentwicklung und Best Practices“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Menas Saweha, Rona Paca
Gastreferent: Vertreterin der Österreichischen Datenschutzbehörde

12. November 2024, 9:15 – 17:00 Uhr:

„Updates zur praktischen Anwendbarkeit und Use-Cases“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, 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.

3. Updates aus der EU

EDSA-Leitlinien zum berechtigten Interesse

Die Definition des „berechtigten Interesses“ gemäß Artikel 6 Absatz 1 lit. f der Datenschutz-Grundverordnung (DSGVO) war seit deren Einführung häufig Gegenstand von Diskussionen. Insbesondere für das Verhältnis zwischen Unternehmen und Privatpersonen ist es entscheidend, zu klären, wann Daten auf dieser Grundlage verarbeitet werden dürfen. Aus diesem Grund ist es begrüßenswert, dass der Europäische Datenschutzausschuss (EDSA) Leitlinien[5] zu diesem Thema veröffentlicht hat.

Die Leitlinien machen deutlich, dass die Datenverarbeitung auf Basis des berechtigten Interesses nicht nur als „letzter Ausweg“ angesehen werden sollte, wenn andere Rechtsgrundlagen nicht greifen. Gleichzeitig wird betont, dass diese Rechtsgrundlage nicht übermäßig ausgeweitet werden darf, nur weil sie als weniger einschränkend wahrgenommen wird als andere Verarbeitungsgrundlagen. Die EDSA-Leitlinien sollen somit helfen, ein ausgewogenes Verständnis für den Umgang mit personenbezogenen Daten im Rahmen berechtigter Interessen zu fördern.

Cyber Resilience Act vom Rat angenommen

Der Cyber Resilience Act[6] wurde am 10. Oktober vom Rat der EU-Innenminister angenommen. Er gilt für Produkte mit digitalen Elementen und stellt sicher, dass vernetzte Produkte wie Kameras, Kühlschränke und Spielzeug sicher sind, bevor sie auf den Markt kommen. Ziel ist es, bestehende Lücken zu schließen, die Rechtsvorschriften klarer zu definieren und die Cybersicherheitsvorschriften einheitlicher zu gestalten.

Die Kernpunkte der EU-Verordnung umfassen verbindliche Cybersicherheitsanforderungen für alle vernetzten Geräte sowie ein verpflichtendes CE-Kennzeichen, das als Indikator für die Cybersicherheit dienen soll. Betroffen von diesen Regelungen sind Hersteller, Importeure und Händler. Zudem wird eine Meldepflicht für Schwachstellen eingeführt und die Erforderlichkeit von regelmäßigen Sicherheitsupdates.

Nach der Unterzeichnung des Cyber Resilience Acts durch die Präsidenten des Rates und des Europäischen Parlaments wird er im Amtsblatt der EU veröffentlicht. Die neue Verordnung tritt 20 Tage nach dieser Veröffentlichung in Kraft und gilt 36 Monate nach Inkrafttreten, wobei einige Bestimmungen bereits früher Anwendung finden werden.

4. Neues aus der Rechtsprechung

EuGH erleichtert Mitbewerbern die Durchsetzung von DSGVO-Verstößen

Am 4. Oktober 2024 fällte der EuGH in der Rechtssache C-21/23[7] ein wegweisendes Urteil zur Verarbeitung von Gesundheitsdaten beim Online-Verkauf von apothekenpflichtigen Arzneimitteln. Die Entscheidung ist von erheblicher Bedeutung für die gesamte Pharmabranche und den Datenschutz.

[5] **https://kurzlinks.de/08zk**
[6] **https://kurzlinks.de/wbl6**
[7] **https://kurzlinks.de/t9zy**

Hintergrund des Falls

Ein niedergelassener Apotheker klagte gegen einen Wettbewerber, der neben einem stationären Geschäft auch Arzneimittel über das Internet vertreibt. Der Kläger warf dem Wettbewerber vor, unzulässig Gesundheitsdaten zu verarbeiten, was gegen die DSGVO verstoße und damit einen unlauteren Wettbewerb darstelle. Der Fall wurde zunächst vom Landgericht Dessau-Roßlau und später vom OLG Naumburg entschieden, die beide zugunsten des Klägers entschieden.

Angesichts dieser Entscheidungen wandte sich der Bundesgerichtshof an den EuGH, um Klarheit über zwei zentrale Fragen zu erhalten:

1) Ist es im Rahmen der DSGVO möglich, Klagen gegen Wettbewerber wegen Datenschutzverletzungen auf das Wettbewerbsrecht zu stützen?
2) Werden auch nicht verschreibungspflichtige Arzneimittel als Gesundheitsdaten betrachtet?

Wesentliche Entscheidungen des EuGH

Das Gericht stellte fest, dass die bei der Online-Bestellung eingegebenen Daten als Gesundheitsdaten im Sinne der DSGVO gelten. Die Begründung des EuGH besagt, dass aus diesen Informationen durch gedankliche Kombination Rückschlüsse auf den Gesundheitszustand einer identifizierten oder identifizierbaren Person gezogen werden können. Dies gilt unabhängig davon, ob die Daten sich auf den Käufer selbst oder auf eine andere Person beziehen, für die die Bestellung aufgegeben wird.

Das Gericht stellte zudem fest, dass die DSGVO der nationalen Regelung, die unlautere Geschäftspraktiken verbietet, nicht im Weg steht. Es bestehe die Möglichkeit, gemäß dem Gesetz gegen den unlauteren Wettbewerb (UWG) zu klagen, denn dies ergänze die Aufsicht und Durchsetzung der DSGVO durch die zuständigen Behörden.

Fazit: Das Urteil des EuGH hat weitreichende Konsequenzen für den Online-Verkauf von Arzneimitteln und den Datenschutz in der Pharmabranche. Es stellt sicher, dass die Verarbeitung von Gesundheitsdaten hohen Schutz genießt und dass alle Akteure im Gesundheitssektor verantwortungsbewusst mit Daten der Kunden umgehen müssen. Apotheker, die online verkaufen, sind nun verpflichtet, umfassende Informationen zur Datenverarbeitung bereitzustellen und die Einwilligung der Kunden einzuholen. Gleichzeitig stärkt die Entscheidung den fairen Wettbewerb.

5. Top Bußgelder

1. Öffentlich zugängliche Ordner in Teams

Die Universität Agder in Norwegen speicherte seit August 2018 personenbezogene Daten in öffentlich zugänglichen Ordnern auf Microsoft Teams, was dazu führte, dass auch Mitarbeitende ohne direkten beruflichen Bedarf auf diese Informationen zugreifen konnten. Betroffen waren etwa 16.000 Personen, darunter Angestellte, Studierende und externe Personen. In den Ordnern waren teilweise hochsensible Daten wie Namen, nationale Identitätsnummern, Prüfungsergebnisse, Prüfungsversuche, Sonderregelungen sowie Kontaktdaten und Informationen zum Aufenthaltsstatus ukrainischer Flüchtlinge enthalten.

Aufgrund der Verletzung von Art. 24 und 32 der DSGVO wurde die Universität mit einem Bußgeld von EUR 12.565[8] belegt. Die Universität

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

hätte geeignete technische und organisatorische Maßnahmen (TOM) einführen müssen, um den Zugriff auf die Daten zu beschränken. Obwohl bei der Auswahl der Maßnahmen Spielraum verbleibt, wäre zumindest ein Berechtigungskonzept erforderlich gewesen, um unberechtigte Zugriffe zu verhindern.

2. Nicht anonymisierte Gesundheitsdaten

Die französische Datenschutzbehörde CNIL[9] verhängte wegen zweier Datenschutzverstöße eine Geldstrafe von EUR 800.000 gegen ein Unternehmen, das Ärztesoftware entwickelt.

Das Unternehmen nutzte ohne Genehmigung nicht-anonymisierte Gesundheitsdaten für Studien und Statistiken. Diese Daten beinhalteten sensible Informationen wie Geburtsjahr, Geschlecht, Krankengeschichte, Allergien und ärztliche Verschreibungen. Laut französischem Recht dürfen solche personenbezogenen Gesundheitsdaten nur mit Genehmigung der CNIL oder nach bestimmten Vorgaben verarbeitet werden.

Zusätzlich speicherte die Software automatisch Daten aus dem Teledienst „HRi" der Krankenversicherung in der Patientenakte. Dies erfolgte jedes Mal, sobald der Arzt eine Abfrage startete, unabhängig davon, ob der Arzt die Daten tatsächlich für relevant hielt. Dieser Automatismus verstößt gegen Art. 5 Abs. 1 lit. a DSGVO, der vorschreibt, dass Daten nur rechtmäßig verarbeitet werden dürfen. Die CNIL betonte, dass dies nur der Fall ist, wenn die Entscheidung über das Speichern beim Arzt verbleibt.

3. Datenschutzverstoß einer Schönheitsklinik

Eine spanische Schönheitsklinik nutzte Vorher-Nachher-Fotos einer Patientin in sozialen Netzwerken zu Werbezwecken, ohne zuvor deren Einwilligung einzuholen. Die Fotos wurden vom behandelnden Chirurgen aufgenommen, der die Patientin operiert hatte, allerdings nicht in der Klinik selbst. Die Klinik verwaltete jedoch die Patientendaten und veröffentlichte die Fotos, um für die Dienstleistungen des Arztes zu werben, weshalb sie für den Vorfall verantwortlich gemacht wurde.

Die spanische Datenschutzbehörde (AEPD)[10] verhängte ein Bußgeld von EUR 10.000, da die Klinik gegen Art. 6 und 9 DSGVO verstoßen hatte. Zwar hatte die Patientin zugestimmt, dass Fotos zu Dokumentationszwecken angefertigt werden, jedoch keine Einwilligung für deren Veröffentlichung in sozialen Medien erteilt. Da diese Nutzung zu Werbezwecken erfolgte, handelte die Klinik ohne rechtliche Grundlage.

Dieser Fall zeigt, dass die Verwendung von Fotografien bereits bei der Einwilligung klar abgegrenzt werden muss – in diesem Fall zwischen Dokumentation und Werbung.

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

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

Erfüllung der Pflichten der NIS-2-Richtlinie: Unsere Beratungsangebot

Ab voraussichtlich Oktober 2024 wird in Österreich ein neues Gesetz für Informationssicherheit (NISG 2024) in Kraft treten, das deutlich mehr Unternehmen betrifft als sein Vorgänger.

Unternehmen müssen sich auf umfassende neue Anforderungen einstellen, um die Sicherheit ihrer Netz- und Informationssysteme zu gewährleisten. Unsere Beratung steht Ihnen zur Seite, um diese Herausforderungen erfolgreich zu meistern.

Wichtige Pflichten des neuen Gesetzes:

- **Risikomanagement**: Unternehmen müssen Risiken für ihre IT-Systeme analysieren und geeignete Maßnahmen zur Risikominimierung ergreifen.
- **Vorfallmeldung**: Sicherheitsvorfälle, die den Betrieb beeinträchtigen könnten, müssen unverzüglich gemeldet und zügig behoben werden.
- **Krisenmanagement**: Pläne zur Wiederherstellung und Minimierung von Ausfällen müssen entwickelt und regelmäßig getestet werden.
- **Informationsaustausch**: Unternehmen sind verpflichtet, mit Behörden und Partnern zusammenzuarbeiten und Informationen über Bedrohungen und Vorfälle auszutauschen.
- **Lieferkettensicherheit**: Auch die Sicherheit von Lieferanten und Drittanbietern muss überwacht und sichergestellt werden.
- **Compliance**: Alle Maßnahmen müssen dokumentiert werden und nachweislich den gesetzlichen Vorgaben entsprechen.

Unsere Beratung unterstützt Sie in allen Bereichen:

- **Individuelle Risikobewertungen**: Wir analysieren Ihre spezifischen Risiken und entwickeln maßgeschneiderte Sicherheitskonzepte, die den Anforderungen des NIS 2 Gesetzes gerecht werden.
- **Effektives Vorfallmanagement**: Wir helfen Ihnen, ein effizientes Vorfallmanagement aufzubauen und unterstützen Sie bei der Einhaltung der strengen Meldepflichten.
- **Krisen- und Wiederherstellungsplanung**: Wir entwickeln robuste Krisenpläne und Wiederherstellungsstrategien, die sicherstellen, dass Ihr Betrieb im Ernstfall schnell lauffähig gemacht wird.
- **Umfassende Schulungen**: Wir bieten Schulungen und Sensibilisierungsprogramme an, um Ihr Team auf die neuen Anforderungen vorzubereiten und die Cybersicherheitskultur in Ihrem Unternehmen zu stärken.
- **Dokumentation und Compliance**: Wir unterstützen Sie bei der Erstellung und Pflege der erforderlichen Dokumentation, um sicherzustellen, dass Sie jederzeit nachweisen können, dass Sie alle gesetzlichen Vorgaben erfüllen.

Unser umfassendes wissenschaftliches Know-how und unser praxisorientierter Ansatz machen uns zum idealen Partner für die Umsetzung der NIS-2-Anforderungen. Mit unserer Unterstützung sind Sie bestens vorbereitet, um die neuen gesetzlichen Pflichten effizient und nachhaltig zu erfüllen.

Kontaktieren Sie uns für eine individuelle Beratung und lassen Sie uns gemeinsam Ihre IT-Sicherheitsziele erreichen!