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 2025 Ausgabe Nr. 117

Liebe Leserinnen und Leser,

der Datenschutz bleibt ein dynamisches Feld, das stetig neue Entwicklungen mit sich bringt. In dieser Ausgabe unseres Newsletters beleuchten wir gleich mehrere bedeutende Neuerungen, die Sie in Ihrer täglichen Arbeit berücksichtigen sollten.

Ein zentrales Thema ist das neue Informationsfreiheitsgesetz, das mehr Transparenz in der Verwaltung ermöglichen soll; wir liefen einen kompakten Überblick. Weitere Themen sind das nun geltende Faxverbot im Gesundheitswesen, sowie die neuen EDSA-Leitlinien zur Pseudonymisierung. Diese liefern wertvolle Impulse für die praktische Umsetzung und zeigen, wie Unternehmen und Behörden Daten so verarbeiten können, dass das Risiko für Betroffene minimiert wird.

Im April informieren wir Sie im Rahmen unseres diesjährigen Datenschutz-Praxisseminars über aktuelle Entwicklungen und Best Practices. Nähere Infos finden Sie hier und in unserer DSG-Info.

Mag. Judith Leschanz
Geschäftsführung

1. Das neue Informationsfreiheitsgesetz

Die Implementierung des Informationsfreiheitsgesetzes[1] (IFG) ab dem 1. September 2025 läutet eine signifikante Transformation in Bezug auf Transparenz und Bürgerrechte in Österreich ein. Die Abschaffung des Amtsgeheimnisses, das ein Jahrhundert lang den Zugang zu staatlichen Informationen maßgeblich erschwert hat, stellt einen grundlegenden Wandel dar.

Von der Amtsverschwiegenheit zur Transparenzpflicht

Die im neuen Art. 22a B-VG verankerte Transparenzpflicht umfasst sowohl eine proaktive Informationspflicht als auch ein Grundrecht auf Zugang zu Informationen. Das IFG normiert eine Verpflichtung zur **proaktiven Veröffentlichung**, der u.a. Legislative, Verwaltungsbehörden und Gerichte unterliegen.

Diese Verpflichtung besteht allerdings nicht für Gemeinden unter 5.000 Einwohnern. Ebenso sind private Stellen wie Stiftungen, Fonds und Unternehmen, die der Kontrolle des Rechnungshofes oder eines Landesrechnungshofes unterliegen, davon ausgenommen, aber sie sind verpflichtet, **auf Anfrage** Zugang zu den entsprechenden Informationen zu gewähren. Diese Regelung bringt Österreich in Einklang mit internationalen Standards, stellt jedoch auch Herausforderungen hinsichtlich des

[1] https://kurzlinks.de/4a0n

Datenschutzes und der praktischen Umsetzung dar.

Ein Fortschritt mit Einschränkungen

Weiterhin der Geheimhaltungspflicht unterliegen Informationen, die für die nationale Sicherheit, die außenpolitischen Interessen, die Abwehr wirtschaftlicher Schäden für Gebietskörperschaften, die Vorbereitung von Entscheidungen sowie die Wahrung berechtigter Interessen anderer erforderlich sind.

Die Datenschutzbehörde (DSB) hat die Aufgabe, die Organe bei der praktischen Umsetzung der vorgesehenen Interessensabwägung zwischen Informationsfreiheit und Datenschutz zu beraten. Die Entscheidung zwischen dem öffentlichen Interesse und dem Recht auf Schutz der persönlichen Daten muss jedoch immer im Einzelfall getroffen werden.

Für private Stellen ist es von besonderer Wichtigkeit, im Vorfeld zu klären, in welchen Fällen der Zugang zu Informationen verweigert werden kann und rechtzeitig Unsicherheiten auszuräumen. Antragsteller können sich zur Berufung an das zuständige Bundes- oder Landesverwaltungsgericht wenden, wenn sie mit der Beantwortung nicht einverstanden sind. Für die Verweigerung einer Information muss die betroffene Stelle daher eine stichhaltige und nachvollziehbare Begründung liefern.

Praktische Umsetzung und Herausforderungen

Die Handhabung von Anfragen erweist sich als komplexes Problem. Eine Entscheidungsfrist von vier Wochen ist vorgesehen, die in Ausnahmefällen verlängert werden kann. Ein klar definierter Arbeitsablauf ist in diesem Zusammenhang unerlässlich. Die vorgesehene Möglichkeit, den Zugang zu Informationen durch Beschwerde bei einem Verwaltungsgericht zu erzwingen, macht es notwendig, jede Auskunftsverweigerung fundiert zu begründen und zu dokumentieren.

Fazit

Zusammenfassend lässt sich festhalten, dass das IFG einen vielversprechenden Anfang darstellt, jedoch noch Verbesserungspotenzial aufweist. Der Erfolg des Gesetzes wird davon abhängen, inwiefern die Regierung Transparenz ernsthaft verfolgt. Ein ambitionierter erster Schritt ist getan, doch es bleibt abzuwarten, ob sich das IFG als wirksames Instrument oder als halbherzige Reform erweist.

Kontaktieren Sie uns, um herauszufinden, ob Sie vom IFG betroffen sind!

IFG Compliance Paket

Das **Informationsfreiheitsgesetz (IFG)** wurde am 31. Jänner 2024 im Nationalrat beschlossen und tritt am **1. September 2025 in Kraft**. Es markiert einen bedeutenden Schritt hin zu mehr Transparenz in Österreich und löst das bisher geltende Amtsgeheimnis weitgehend ab. Es wird ein **moderner rechtlicher Rahmen** für den Zugang zu Informationen geschaffen und das Vertrauen in staatliche Institutionen durch eine **offene und transparente Verwaltung** gestärkt.

Unser **IFG Compliance-Paket** unterstützt Sie umfassend bei der **Umsetzung** der gesetzlichen Vorgaben und sorgt dafür, dass Ihre Organisation **optimal vorbereitet** ist. Unsere Expertise vereint rechtliches Know-how, strategische Beratung und praxisnahe Lösungen.

Unsere Leistungen im Überblick:

- **Prozesse & Workflows:** Analyse interner Anlaufstellen, Definition klarer Zuständigkeiten und Entwicklung effizienter Abläufe für Anträge nach dem Informationsfreiheitsgesetz

- **Schulung & Richtlinien:** Erstellung praxisnaher Schulungsunterlagen und Checklisten zur schnellen Antragsprüfung
- **Antragsbearbeitung:** Beratung zu Antwortstrategien und Bereitstellung von Musterdokumenten für unterschiedliche Szenarien
- **Dokumentation & Compliance:** Entwicklung klarer Vorgaben zur Erfassung und Kategorisierung von Informationen
- **Strategische Beratung:** Unterstützung bei der Begründung von Ausnahmen und der Interessenabwägung

Ihre Vorteile:

- ✓ **Sicherheit:** Minimierung von Verfahrensrisiken durch klare Prozesse und strukturierte Dokumentation
- ✓ **Effizienz:** Optimierte Workflows für die schnelle und einheitliche Bearbeitung von IFG-Anfragen
- ✓ **Mitarbeiterschulung:** Sensibilisierung und Qualifizierung Ihres Teams für den professionellen Umgang mit Anträgen nach dem Informationsfreiheitsgesetz

2. Faxverbot im Gesundheitswesen sorgt für Chaos

Seit dem 1. Jänner 2025 ist in Österreich die Übermittlung von Gesundheitsdaten per Fax nicht mehr zulässig. Dieses Verbot wurde aufgrund von Datenschutzbedenken eingeführt, da Faxgeräte als unsichere Kommunikationsmittel gelten und nicht den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprechen. Die Umsetzung dieser Regelung, welche bereits im BGBl. vom 19. Juli 2024 verlautbart wurde, hat jedoch zu erheblichen Kommunikationsproblemen im Gesundheitswesen geführt.

Bisher wurden nach wie vor viele Dokumente, darunter Rezepte, Überweisungen und Befunde, per Fax übermittelt. Da Alternativen wie verschlüsselte E-Mails oder Plattformen zur verschlüsselten Übermittlung nicht überall verfügbar sind, führt das Verbot zu Verzögerungen und erheblichem bürokratischen Mehraufwand. In einigen Fällen werden CDs oder USB-Sticks physisch zwischen Einrichtungen ausgetauscht, was den Arbeitsablauf erheblich verlangsamt und die Patientenversorgung beeinträchtigt. Besonders betroffen sind ältere oder technisch wenig versierte Ärzte sowie kleine Gesundheitseinrichtungen, die bisher das Fax als zuverlässiges Kommunikationsmittel angesehen haben.

Die **Österreichische Gesundheitskasse** (ÖGK) hat als Reaktion auf das Verbot ein webbasiertes System auf Basis des **Clouddienstes FTAPI** eingeführt, das den sicheren Austausch sensibler Informationen ermöglichen soll. Dieses System stößt jedoch auf Kritik, da es als „hochkomplex in der Anwendung“ gilt und angeblich oft mit bestehenden IT-Systemen nicht kompatibel ist. Als Alternativen zum Fax werden auch verschlüsselte E-Mails, sichere Patientenportale und die Nutzung der elektronischen Gesundheitsakte (ELGA) empfohlen. Diese Lösungen sollen langfristig die sichere und effiziente Kommunikation im Gesundheitswesen gewährleisten.

Fazit

Das Faxverbot sollte den Datenschutz stärken und die Digitalisierung vorantreiben. In der Praxis führt es jedoch zu erheblichen Herausforderungen. Investitionen in sichere digitale Kommunikationswege sind in jedem Fall erforderlich.

3. EDSA-Leitlinien zur Pseudonymisierung

Am 17. Jänner 2025 hat der Europäische Datenschutzausschuss (EDSA) neue Leitlinien zur Pseudonymisierung[2] veröffentlicht. Diese sollen Unternehmen und Organisationen dabei unterstützen, ihre Datenschutzverpflichtungen gemäß der Datenschutz-Grundverordnung (DSGVO) besser zu erfüllen.

Definition und Bedeutung

Die DSGVO definiert Pseudonymisierung als die Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Diese zusätzlichen Informationen müssen getrennt aufbewahrt und durch technische und organisatorische Maßnahmen geschützt werden.

Wichtig ist, dass pseudonymisierte Daten weiterhin als **personenbezogene Daten** gelten und somit den Bestimmungen der DSGVO unterliegen. Dennoch kann die Pseudonymisierung das Risiko für die Rechte und Freiheiten betroffener Personen reduzieren und die Nutzung berechtigter Interessen als Rechtsgrundlage erleichtern.

Vorteile und Anwendung der Pseudonymisierung

Die EDSA-Leitlinien betonen, dass Pseudonymisierung eine effektive Maßnahme sein kann, um

- Datenschutzgrundsätze wie Datenminimierung und Zweckbindung besser einzuhalten,
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu fördern,
- die Sicherheit der Verarbeitung zu erhöhen und das Risiko von Datenschutzverletzungen zu verringern.

Durch den Einsatz von Pseudonymisierung können Unternehmen datenschutzfreundliche Anwendungen entwickeln und gleichzeitig wertvolle Datenanalysen durchführen, insbesondere in datenintensiven Branchen wie dem Finanzwesen, dem Personalmanagement und dem Gesundheitssektor.

Technische Umsetzung

Für eine wirksame Pseudonymisierung empfiehlt der EDSA ein dreistufiges Verfahren:

1. **Transformation der Daten**: Entfernen oder Ersetzen von Identifikatoren durch Techniken wie Verschlüsselung oder Tokenisierung
2. **Trennung und Schutz zusätzlicher Informationen**: Sichere und getrennte Aufbewahrung von Informationen, die zur Re-Identifikation erforderlich sind, wie zB Zuordnungstabellen oder kryptografische Schlüssel
3. **Implementierung technischer und organisatorischer Maßnahmen**: Einsatz von Zugangsbeschränkungen, physische Trennung von Daten und regelmäßige Sicherheitsüberprüfungen, um eine unbefugte Re-Identifikation zu verhindern

[2] https://kurzlinks.de/mbuz

Öffentliche Konsultation und Ausblick

Die Leitlinien werden bis März 2025 einer öffentlichen Konsultation unterzogen, um interessierten Parteien die Möglichkeit zum Feedback zu geben und zukünftige Entwicklungen in der Rechtsprechung zu berücksichtigen.

Obwohl die Leitlinien des EDSA nicht rechtlich bindend sind, dienen sie als wichtige Orientierungshilfe für Unternehmen und Aufsichtsbehörden bei der Umsetzung und Auslegung der DSGVO. Unternehmen sind daher gut beraten, Empfehlungen des EDSA konsequent umzusetzen und ihre internen Prozesse regelmäßig zu überprüfen, um der Weiterentwicklung der datenschutzrechtlichen Anforderungen gerecht zu werden.

4. Bußgelder

1. Cyberangriff auf Versicherungsgesellschaft

Die spanische Versicherungsgesellschaft Generali España wurde Opfer eines Cyberangriffs, bei dem Hacker Zugriff auf personenbezogene Daten ehemaliger Kunden erhielten. Betroffen waren unter anderem Namen, Geburtsdaten, Ausweiskopien, Adressen, Telefonnummern, E-Mail-Adressen und Bankverbindungen.

Der Angriff wurde bereits im September 2022 durchgeführt, jedoch erst im Oktober entdeckt. Die Angreifer nutzten die Zugangsdaten eines Versicherungsmaklers, um sich in ein Kundenportal einzuloggen und dort automatisiert Daten auszulesen. Zwar wurde das betroffene Benutzerkonto am 6. Oktober 2022 gesperrt, jedoch erfolgte keine sofortige Meldung an die Datenschutzbehörde. Erst im November 2022 stellte sich heraus, dass die gestohlenen Daten bereits über eine Telegram-Gruppe verkauft wurden. Insgesamt waren über 1,6 Millionen Kunden betroffen.

Die spanische Datenschutzbehörde (AEPD) verhängte daraufhin eine Geldstrafe in Höhe von 4 Mio. Euro.[3] Generali España wurde unter anderem Verstöße gegen Art. 5, 25, 32 und 35 DSGVO zur Last gelegt.

Dieser Fall zeigt, wie wichtig die schnelle Reaktion auf Cyberangriffe ist. Unternehmen müssen nicht nur angemessene Sicherheitsmaßnahmen implementieren, sondern auch über geeignete Prozesse die Erkennung und Meldung von Datenschutzverstößen sicherstellen.

2. Datenschutzverstoß bei Orange Romania

Die rumänische Datenschutzbehörde verhängte ein Bußgeld gegen den Telekommunikationsanbieter Orange Romania,[4] weil das Unternehmen nicht ordnungsgemäß auf Löschanfragen reagierte. Abgelehnte potenzielle Kunden forderten die Löschung ihrer Daten, erhielten jedoch unzureichende Antworten oder mussten unnötige persönliche Informationen bereitstellen. Zudem speicherte Orange personenbezogene Daten, darunter gescannte Dokumente, obwohl diese für den Vertragsabschluss nicht mehr erforderlich waren.

Für diese Verstöße gegen Art. 5, 6, 7 und 12 DSGVO sowie nationale Datenschutzvorschriften wurde eine Strafe von knapp EUR 40.000 verhängt.

Weiterer Verstoß in Frankreich

Bereits im Dezember 2024 wurde die französische Tochter Orange FR von der CNIL mit einem Bußgeld von 50 Mio. Euro[5] belegt. Grund dafür waren Werbeanzeigen im Postfach des firmeneigenen Messenger-Dienstes, die sich optisch an reguläre E-Mails anlehnten und ohne Einwilligung der Nutzer angezeigt wurden. Zudem wurden Cookies trotz Widerruf der Zustimmung weiterhin ausgelesen. Neben der Geldstrafe wurde eine einstweilige Verfügung erlassen: Falls Orange das Cookie-Tracking nach Widerruf nicht innerhalb von drei Monaten einstelle, drohe eine tägliche Strafzahlung von EUR 100.000.

Beide Fälle zeigen, dass Datenschutzverstöße konsequent geahndet werden. Insbesondere die unsachgemäße Bearbeitung von Löschanfragen sowie die unerlaubte Verarbeitung personenbezogener Daten können Unternehmen teuer zu stehen kommen.

Sie unterstreichen auch die Notwendigkeit, Löschkonzepte zeitnah zu aktualisieren, insbesondere vor dem Hintergrund, dass der Europäische Datenschutzausschuss (EDPB) das Recht auf Löschung als zentrales Thema für

[3] https://kurzlinks.de/e8or
[4] https://kurzlinks.de/uymi
[5] https://kurzlinks.de/lcpr

2025 festgelegt hat. Die österreichische Datenschutzbehörde wird diese Kontrollen im Rahmen eines amtswegigen Prüfverfahrens durchführen. Die betroffene Branche ist noch nicht bekannt.

3. Datenschutzverstöße bei OpenAI: 15-Millionen-Euro-Bußgeld

Die italienische Datenschutzbehörde hat OpenAI mit einem Bußgeld von 15 Mio. Euro[6] belegt. Grund dafür sind mehrere Verstöße gegen die DSGVO beim Betrieb des Chatbots ChatGPT.

Die Ermittlungen begannen nach Bekanntwerden einer Datenschutzverletzung, die nicht fristgerecht gemeldet wurde. Im Verlauf der Untersuchung stellte die Behörde weitere Verstöße fest, insbesondere gegen die Grundsätze der Rechtmäßigkeit, Transparenz und Richtigkeit.

Nach Auffassung der Behörde versäumte OpenAI, vor der Inbetriebnahme von ChatGPT eine gültige Rechtsgrundlage für die Datenverarbeitung zum Training ihres Large Language Models festzulegen. Zudem wurde kritisiert, dass die Datenschutzerklärung unzureichend war – insbesondere in Bezug darauf, wie Betroffene, die den Dienst nicht selbst nutzen, über die Verarbeitung ihrer Daten informiert werden. Auch das Fehlen einer Altersverifikation und die unzureichende Umsetzung einer vorhergehenden behördlichen Anordnung wurden beanstandet.

Der Fall beleuchtet verschiedene datenschutzrechtliche Fragestellungen im Zusammenhang mit der Verarbeitung von Daten durch KI-Modelle. Besonders brisant ist die Bewertung der von OpenAI bereitgestellten Informationsmaterialien, darunter Pop-Ups, Artikel im Hilfecenter und Forschungsberichte. Die Behörde stufte diese als nicht ausreichend ein, um den Anforderungen der DSGVO zu genügen. Noch offen bleibt die Frage, ob das berechtigte Interesse als Rechtsgrundlage für das Training der KI zulässig ist, und wie das Phänomen des „Halluzinierens“ als Verstoß gegen den Grundsatz der Richtigkeit einzuordnen ist. Aufgrund möglicher laufender Verstöße wurde der Fall an die irische Datenschutzbehörde weitergeleitet.

PS.: Am 27. Dezember 2024 bestätigte das Bundesverwaltungsgericht (BVwG) die Geldstrafe von 16 Mio. Euro gegen die Österreichische Post AG aufgrund von Datenschutzverletzungen. Die Post hatte ohne ausreichende Rechtsgrundlage Daten zur Parteiaffinität von Kunden verarbeitet und weiterverkauft.

Save the Date – Privacy Ring

Der Datenschutzverein Privacy Ring[7] lädt am **13. März 2025** zur inzwischen 13. Fachtagung in Rotkreuz, Schweiz ein. Diesmal steht das Thema **Datenschutz @AI – Technologisches Verständnis und datenschutzrechtliche Herausforderungen** im Fokus. Die Veranstaltung kann auch online mitverfolgt werden. Der Zoom-Link für die **Online-Teilnahme** wird den Teilnehmenden vor der Veranstaltung zugesendet.

Im Anschluss werden mit verschiedenen Expertinnen und Experten aus der Wirtschaft und dem öffentlichen Bereich eine Podiumsdiskussion sowie ein Get-together abgehalten.

[6] https://kurzlinks.de/wpmz

[7] https://www.privacy-ring.uni-hannover.de/de/