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 2025 Ausgabe Nr. 118

Liebe Leserinnen und Leser,

der Datenschutz bleibt ein zentrales Thema in der digitalen Welt und auch in dieser Ausgabe unseres Newsletters werfen wir einen Blick auf aktuelle Entwicklungen und praxisrelevante Entscheidungen.

Ein besonderes Highlight war unser Datenschutz-Praxisseminar 2025, das wieder einmal wertvolle Einblicke und praxisnahe Diskussionen bot. Expertinnen und Experten aus Wirtschaft, Verwaltung und Recht teilten ihre Erfahrungen und stellten Best Practices vor, um den Herausforderungen der DSGVO gerecht zu werden.

Ein weiterer Schwerpunkt dieser Ausgabe liegt auf dem diesjährigen amtswegigen Prüfverfahren der österreichischen Datenschutzbehörde. Diesmal steht die Einhaltung datenschutzrechtlicher Vorgaben durch die Landespolizeidirektionen im Fokus.

Abgerundet wird unser Newsletter mit einer Übersicht über aktuelle Entscheidungen zum Datenschutz. Sie verdeutlichen einmal mehr, wie dynamisch sich die Rechtslage entwickelt und welche Konsequenzen das für Unternehmen und öffentliche Stellen hat.

Wir wünschen Ihnen eine spannende Lektüre und freuen uns auf den weiteren Austausch!

Mag. Judith Leschanz
Geschäftsführung

1. Rückblick auf das Datenschutz-Praxisseminar 2025

Das kürzlich abgehaltene Datenschutz-Praxisseminar der Secur-Data bot Fach- und Führungskräften eine umfassende Schulung zur Datenschutz-Grundverordnung (DSGVO) und der praktischen Umsetzung datenschutzrechtlicher Vorgaben. Die Veranstaltung richtete sich insbesondere an Datenschutzbeauftragte, IT-Manager, Compliance-Beauftragte, Juristen und Unternehmensberater.

Seminarinhalte und Schwerpunkte

Das Seminar gliederte sich in zwei thematische Blöcke. Der erste Tag konzentrierte sich auf rechtliche Entwicklungen sowie bewährte Best Practices. Die Teilnehmenden erhielten eine detaillierte Einführung in die gesetzlichen Anforderungen und wurden über die neuesten nationalen und europäischen Entwicklungen informiert. Besonders die jüngsten Änderungen und ihre Auswirkungen wurden intensiv diskutiert, um ein solides Verständnis für die rechtlichen Rahmenbedingungen herzustellen.

Am zweiten Tag lag der Fokus auf der praktischen Anwendbarkeit von Datenschutzregelungen im Unternehmensalltag. Neben Themen wie Informationssicherheit und technischen und organisatorischen Maßnahmen (TOM) wurde auch das Verfahren vor der

Datenschutzbehörde behandelt. Ein wichtiger Punkt war außerdem die Auseinandersetzung mit der Schnittstelle zwischen DSGVO und Künstlicher Intelligenz (KI), die immer mehr an Bedeutung gewinnt.

Die Teilnehmenden konnten praxisnahes Wissen zur effektiven Umsetzung der DSGVO und zur Stärkung der Datensicherheit erwerben.

Fazit

Die Veranstaltung bot nicht nur wertvolle Einblicke in die aktuelle Rechtssituation, sondern auch praxisnahe Lösungsansätze für den Arbeitsalltag. Frau Mag. Leschanz, Geschäftsführerin der Secur-Data, betonte die Relevanz der laufenden Weiterbildung: „Datenschutz ist keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess. Unser Seminar hilft Unternehmen, sich auf die dynamischen Herausforderungen des Datenschutzes vorzubereiten und innovative Lösungen zu entwickeln."

Mit praxisnahen Fallbeispielen und interaktiven Diskussionen war das Datenschutz-Praxisseminar ein voller Erfolg und unterstrich die Bedeutung einer fundierten Datenschutzstrategie für Unternehmen aller Branchen.

2. Das amtswegige Prüfverfahren

Die österreichische Datenschutzbehörde (DSB) führt jährlich amtswegige Prüfverfahren durch, um die Einhaltung der Datenschutz-Grundverordnung (DSGVO) in verschiedenen Bereichen zu untersuchen. Diese Prüfungen erfolgen unabhängig von Verdachtsmomenten oder Beschwerden und dienen der proaktiven Überprüfung datenschutzrechtlicher Standards.

Schwerpunktprüfung 2025: Landespolizeidirektionen

Die DSB hat für das Jahr 2025 eine Schwerpunktprüfung angekündigt[1], die sich auf die österreichischen Landespolizeidirektionen konzentriert. Das zentrale Augenmerk liegt auf der praktischen Umsetzung des Rechts auf Löschung sowie den Verfahren zur Wahrnehmung der Betroffenenrechte. Dazu haben die europäischen Datenschutzbehörden im Rahmen des „Coordinated Enforcement Framework" (CEF) einen speziellen Fragebogen entwickelt.

Im Rahmen des Verfahrens wird das Verzeichnis der Verarbeitungstätigkeiten untersucht. Über den Fragebogen wird die Position der Behörden zu allgemeinen und speziell sicherheitspolizeilichen Fragen erhoben. Im weiteren Verlauf können mündliche Verhandlungen und sogar Vor-Ort-Prüfungen erfolgen.

Schwerpunktprüfung 2024: Telekommunikationsbranche im Visier

Im Jahr 2024 richtete die DSB ihr Augenmerk auf den Telekommunikationssektor. Zehn Unternehmen wurden hinsichtlich der Einhaltung datenschutzrechtlicher Verpflichtungen geprüft. Der Fokus lag auf allgemeinen Verpflichtungen wie den Grundsätzen der Datenverarbeitung gemäß Art. 5 DSGVO, technischen und organisatorischen Maßnahmen zur Datensicherheit sowie der Übermittlung personenbezogener Daten in Drittländer. Zudem wurde das Auskunftsrecht nach Art. 15 DSGVO im Rahmen des „Coordinated Enforcement Framework" (CEF)[2] überprüft. Die DSB zog eine positive Bilanz[3] und stellte fest, dass der Telekommunikationsbereich die DSGVO erfolgreich in die Geschäftsprozesse integriert hat.

Rückblick auf 2023: Fokus auf den Finanzsektor

Im Jahr 2023 konzentrierte sich die DSB auf den Finanzsektor und überprüfte stichprobenartig

[1] https://kurzlinks.de/mscv
[2] https://kurzlinks.de/gy4b
[3] https://kurzlinks.de/8std

ausgewählte Kreditinstitute. Besonderes Augenmerk lag dabei auf der (Weiter-)Verarbeitung von Bank- und Kontodaten zu Werbezwecken sowie der Rolle der Datenschutzbeauftragten. Die Behörde stellte fest[4], dass die DSGVO in der Praxis angekommen ist und die Branche gut aufgestellt sei. Grobe Verstöße wurden nicht festgestellt, und der Großteil der anschließenden Verfahren wurde kurz danach eingestellt.

[4] **https://kurzlinks.de/ke7z**

3. Übersicht über das Barrierefreiheitsgesetz

Das österreichische **Barrierefreiheitsgesetz (BaFG)**, veröffentlicht am 19. Juli 2023 im Bundesgesetzblatt (BGBl. I Nr. 76/2023)[5], tritt am **28. Juni 2025 in Kraft**. Es dient der Umsetzung der EU-Richtlinie 2019/882, bekannt als „European Accessibility Act", und zielt darauf ab, den barrierefreien Zugang zu bestimmten Produkten und Dienstleistungen zu gewährleisten.

Ziele und Maßnahmen

Über das Barrierefreiheitsgesetz werden folgende Ansätze umgesetzt:

- Festlegung von Barrierefreiheitsanforderungen:
  Das BaFG definiert spezifische Anforderungen für die Barrierefreiheit ausgewählter Produkte und Dienstleistungen.
- Verpflichtung der Unternehmen:
  Unternehmen sind angehalten, nur Produkte und Dienstleistungen auf den Markt zu bringen, die den festgelegten Barrierefreiheitsanforderungen entsprechen.
- Einrichtung einer Marktüberwachung:
  Das Sozialministeriumservice wird als zuständige Behörde eingesetzt, um die Einhaltung der Bestimmungen zu überwachen.

Betroffene Produkte und Dienstleistungen

Das Gesetz betrifft insbesondere folgende Angebote, die in Zukunft barrierefrei umgesetzt werden müssen:

- Computer- und Betriebssysteme
- Bankdienstleistungen, z.B. im Rahmen von Geldautomaten und Online-Banking
- E-Commerce-Dienste und Websites
- Elektronische Kommunikationsdienste

Ausnahmen gibt es für Kleinstunternehmen, die Dienstleistungen anbieten oder erbringen: Wenn sie weniger als zehn Mitarbeiter beschäftigen und einen Jahresumsatz von maximal 2 Millionen Euro erwirtschaften, sind sie von den Verpflichtungen ausgenommen. Außerdem gibt es Einschränkungen für Fälle, in denen die Umsetzung der Barrierefreiheitsanforderungen zu einer grundlegenden Veränderung des Produkts führen oder das Unternehmen unverhältnismäßig belasten würde.

Durchsetzung und Sanktionen

VerbraucherInnen sowie Organisationen wie der Verein für Konsumenteninformation, der Österreichische Behindertenrat, die Arbeiterkammer und die Wirtschaftskammer Österreich haben das Recht, potenzielle Verstöße dem Sozialministeriumservice zu melden. Bei Verstößen können Geldstrafen von bis zu EUR 80.000[6] verhängt werden.

Fazit

Unternehmen sollten ihre Produkte und Dienstleistungen frühzeitig auf die Einhaltung der neuen Barrierefreiheitsanforderungen überprüfen. Gegebenenfalls sind Anpassungen vorzunehmen, um rechtzeitig zum Inkrafttreten des Gesetzes am 28. Juni 2025 vollständig rechtskonform zu sein.

[5] **https://kurzlinks.de/sqca**

[6] **https://kurzlinks.de/tdjc**

4. Bußgelder

1. Fehlende Zugangsbeschränkungen: Hohes Bußgeld gegen CaixaBank S.A.

Die spanische Datenschutzbehörde Agencia Española de Protección de Datos (AEPD) hat gegen die CaixaBank S.A. ein erhebliches Bußgeld in Höhe von 3,5 Mio. EUR[7] verhängt. Hintergrund war ein Datenschutzverstoß im Zusammenhang mit der Offenlegung sensibler Bank- und Finanzdaten.

Eine Kundin der CaixaBank führte mehrere Konten, darunter ein Gemeinschaftskonto mit einer weiteren Mitinhaberin sowie ein Einzelkonto, für das ihre Mutter als Bevollmächtigte eingetragen war. Aufgrund fehlerhafter Zugriffsberechtigungen innerhalb der Bank-App konnte die Mitinhaberin jedoch auch auf das Einzelkonto der Kundin zugreifen, obwohl sie hierfür keine vertragliche Berechtigung hatte.

Nach einer Beschwerde der betroffenen Kundin stellte die AEPD schwerwiegende Mängel im Berechtigungskonzept fest. Dies betraf sowohl die technische Umsetzung der Bank-App als auch die organisatorischen Maßnahmen der Bank zur Zugangskontrolle.

Die CaixaBank wurde wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) sanktioniert, insbesondere gegen die **Art. 5 Abs. 1 lit. f und Art. 32 DSGVO**. Ein wesentlicher Grund für die hohe Strafe war zudem die fehlende Kooperationsbereitschaft der Bank während des Verfahrens.

Dieser Fall verdeutlicht, wie essenziell wirksame technische und organisatorische Maßnahmen (TOM) für den Schutz personenbezogener Daten sind. Besonders ein durchdachtes Berechtigungsmanagement spielt eine zentrale Rolle, wenn es darum geht, unbefugte Zugriffe zu verhindern. Während technische Maßnahmen primär den IT-Bereich betreffen, sind die organisatorischen Vorkehrungen entscheidend für die praktische Umsetzung. Dazu zählen klare Arbeitsanweisungen, eindeutige Zuständigkeiten und die regelmäßige Schulung und Sensibilisierung der Mitarbeitenden.

Ein Verstoß gegen Art. 32 DSGVO kann nicht nur zu empfindlichen Geldstrafen führen, sondern auch Schadensersatzansprüche der Betroffenen nach sich ziehen. Daher sollten Unternehmen ihre Zugriffsrechte kontinuierlich überprüfen und sicherstellen, dass vertrauliche Daten ausschließlich autorisierten Personen zugänglich sind.

2. Bekannte Sicherheitslücke nicht behoben: Hohe Geldstrafe für AHC

Die britische Datenschutzbehörde (ICO) hat ein Bußgeld in Höhe von 3,07 Mio. GBP[8] (ca. 3,68 Mio. EUR) gegen die Advanced Health & Care Division Limited (AHC), eine Tochtergesellschaft der Aston M IDCO Ltd., verhängt. AHC bietet IT-Dienstleistungen für verschiedene Sektoren wie Gesundheitswesen, Rechtsberatung und Bildungswesen an.

Durch einen Hackerangriff wurden personenbezogene Daten von rund 82.000 Personen kompromittiert, einschließlich sensibler Gesundheitsdaten nach Art. 9 DSGVO. Die Angreifer nutzten eine sicherheitskritische Lücke in einer Microsoft-Software, die bereits 2020 von Microsoft und dem National Institute of Standards and Technology (NIST) entdeckt und als hochgefährlich eingestuft wurde. Obwohl Microsoft die nötigen Sicherheitspatches längst bereitgestellt hatte, hatte AHC diese nicht installiert.

Die ICO kritisierte, dass AHC trotz vorhandener Warnungen und Möglichkeiten zur Behebung keine ausreichenden Maßnahmen zur Risiko-

[7] **https://kurzlinks.de/vfau**

[8] **https://kurzlinks.de/j37m**

minimierung ergriffen hatte. Das Unternehmen hätte die Lücke durch regelmäßige Sicherheitsprüfungen und ein effektives Patch-Management problemlos schließen können. Dadurch verstieß AHC gegen die folgenden Vorschriften: **Art. 5 Abs. 1 lit. f, Art. 9, Art. 32 DSGVO und Art. 32 Abs. 1 UK GDPR.**

Dieser Vorfall verdeutlicht, wie gefährlich Cyberangriffe sind, und wie wichtig die regelmäßige Wartung und Behebung von Schwachstellen. Unternehmen müssen sicherstellen, dass sie über ein wirksames Informationssicherheits-Managementsystem (ISMS) verfügen. Auch die regelmäßige Sensibilisierung der Mitarbeitenden kann entscheidend beitragen, Sicherheitslücken zu schließen und datenschutzrechtliche Verstöße zu vermeiden.

3. Unrechtmäßige Datenverarbeitung und -weitergabe: Hohe Strafe für Poczta Polska

Im Zentrum eines aktuellen Datenschutzvorfalls steht der polnische Postdienstleister Poczta Polska. Im Rahmen der Vorbereitung auf die Präsidentschaftswahl 2020 wurde er vom polnischen Ministerium für Digitalisierung mit der Bereitstellung eines elektronischen Systems zur Registrierung der Bevölkerung beauftragt. Dabei wurden nicht nur PESEL-Daten (vergleichbar mit der Steuer-Identifikationsnummer in Österreich), sondern auch Namen, Adressen und Informationen zu Auslandsreisen der Bürger verarbeitet. Diese Daten wurden zuvor vom Ministerium an Poczta Polska weitergegeben.

Insgesamt gingen 178 Beschwerden von Privatpersonen bei der polnischen Datenschutzbehörde, dem Urząd Ochrony Danych Osobowych (UODO), ein. Die Behörde stellte fest, dass die Weitergabe eines Großteils der Daten an Poczta Polska unrechtmäßig war und in vielen Fällen keine rechtliche Grundlage für die Datenverarbeitung und -weitergabe vorlag. Besonders der Grundsatz der Erforderlichkeit sei häufig nicht beachtet worden. Als Konsequenz wurde gegen Poczta Polska ein Bußgeld von 27.124.816 PLN[9] (ca. 6,48 Mio. EUR) verhängt. Auch das Ministerium für Digitalisierung erhielt ein Bußgeld von 100.000 PLN (ca. EUR 4.000). Die Verstöße betrafen insbesondere **Art. 5 Abs. 1 lit. a und Art. 6 Abs. 1 DSGVO.**

Dieser Vorfall verdeutlicht erneut, wie entscheidend es ist, dass die Verarbeitung und Weitergabe von Daten stets auf einer gültigen Rechtsgrundlage beruht. Das Ministerium für Digitalisierung und Poczta Polska hätten dieses grundlegende Datenschutzprinzip unbedingt beachten müssen. Insbesondere der Grundsatz der Datenminimierung ist von zentraler Bedeutung: Es dürfen nur diejenigen Daten verarbeitet oder weitergegeben werden, die für den konkreten Zweck erforderlich sind. Werden Daten über diesen Zweck hinaus verarbeitet, können sich Verantwortliche mit erheblichen rechtlichen Konsequenzen konfrontiert sehen.

[9] **https://kurzlinks.de/56yb**

••••

KI MADE IN AUSTRIA – Chancen, Herausforderungen & Zukunftsperspektiven

Künstliche Intelligenz verändert Wirtschaft und Gesellschaft. Doch welche Chancen ergeben sich für Unternehmen in Österreich, und welche Herausforderungen müssen bewältigt werden? Das Event *KI Made in Austria* bietet eine exklusive Gelegenheit, sich über bahnbrechende KI-Technologien und die neuesten regulatorischen Anforderungen zu informieren! Gemeinsam mit Secur-Data und dem österreichischen KI-Anbieter goodguys GmbH beleuchtet die Österreichische Computer Gesellschaft:

- AI-Act im Fokus – ExpertInnen erklären die neuesten regulatorischen Entwicklungen und ihre Auswirkungen auf österreichische Unternehmen.
- Revolutionäre KI in der Praxis – Der österreichische KI-Pionier präsentiert eine wegweisende Innovation und zeigt, wie sie DSGVO-konform Branchen transformiert.

Neben spannenden Fachvorträgen und Diskussionen bietet die Veranstaltung Networking-Möglichkeiten mit Branchenführern. *KI Made in Austria* richtet sich an Unternehmen, Start-ups und EntscheidungsträgerInnen, die die Zukunft aktiv mitgestalten wollen.

Die Veranstaltung findet am **7. Mai 2025** ab **16:00 Uhr** in der **OCG**, Wollzeile 1, 1010 Wien statt.

Zur Anmeldung:
www.ocg.at/veranstaltungen/ki-made-austria-chancen-herausforderungen-zukunftsperspektiven

Save the Date – Privacy Ring Wien 2025

Der **14. Privacy Ring** findet am **18. September 2025** in **Wien** statt! Weitere Details folgen in Kürze auf der Secur-Data Website und in unserer DSG-Info!