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

Dezember 2020 Ausgabe Nr. 97

Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!

Das Jahr neigt sich dem Ende zu und wir bedanken uns für die Zusammenarbeit mit Ihnen.

Aus datenschutzrechtlicher Sicht kam es zu einigen Paukenschlägen durch Entscheidungen der Datenschutzbehörden und Gerichte.

Wir möchten Ihnen einen Überblick über die wichtigsten Entscheidungen geben.

Ihren Familien und Mitarbeitern wünschen wir erholsame Feiertage und ein gesundes neues Jahr 2021!

1. Europa

Der Europäische Gerichtshof hat dieses Jahr viele richtungsweisende Entscheidungen getroffen, die von immenser wirtschaftlicher Bedeutung sind.

Das vielseits bekannte Schrems II-Urteil[1] ist die wohl wichtigste gerichtliche Entscheidung des Jahres. Es hat dazu geführt, dass die Übermittlung von Daten in die USA auf Grundlage des Privacy-Shield-Abkommens nicht mehr zulässig ist. Hierzu wurde der europäische Gesetzgeber am 12. November 2020 tätig und hat einen Entwurf für neue Standardvertragsklauseln veröffentlicht, die die Datenübermittlung in Drittländer neu regeln sollen.

Auch der Europäische Datenschutzausschuss hat Empfehlungen[2] zur Einhaltung des EU-Datenschutzniveaus herausgegeben. Der wichtigste Aspekt ist dabei, stets zu wissen, welche Datenübermittlungen stattfinden („*know your transfer*“)[3] und auf welcher Basis diese vorgenommen werden (u.a. Angemessenheitsbeschluss, Standardvertragsklauseln, Binding Corporate Rules). Dies hat gemäß einer Einzelfallbeurteilung zu erfolgen („*case-by-case basis*“).[4]

Gelingt es nicht, ausreichende Maßnahmen zur Einhaltung des EU-Schutzniveaus zu treffen, ist eine Übermittlung nicht zulässig und bestehende Datenverarbeitungsprozesse müssen gestoppt werden („*promptly suspend or end the transfer of personal data*“)[5].

[1] EuGH 16.7.2020, C-311/18 – Schrems II.
[2] *EDPB*, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
[3] *EDPB*, Recommendations 01/2020, Rn. 65.
[4] *EDPB*, Recommendations 01/2020, Rn. 66.
[5] *EDPB*, Recommendations 01/2020, Rn. 67.

Aufsichtsbehörden sind ermächtigt[6], Datenübermittlungen in Drittländer ohne ausreichendes Schutzniveau auszusetzen oder zu stoppen.

Die neuen Dokumente verschärfen die aktuelle Unsicherheit bei der Verwendung von Diensten von Facebook oder Google Analytics noch, da diese Anbieter bisher keine ausreichenden Maßnahmen getroffen haben, um die Einhaltung des EU-Schutzniveaus zu gewährleisten.

Immerhin hat Microsoft aber mit Stand 9. Dezember 2020 zusätzliche Sicherheitsvorkehrungen als Addendum zu den Standardvertragsklauseln veröffentlicht.

EuGH-Urteil zu Orange Romania C-61/19

Der europäische Gerichtshof bestärkt seine strenge Linie zur datenschutzrechtlichen Einwilligung und dem Verbot von Opt-out-Mechanismen.

Mit seinem Urteil[7] hat der EuGH die **strengen Voraussetzungen** der datenschutzrechtlichen Einwilligung bestätigt. Ein rumänischer Telekommunikationsanbieter forderte beim Abschluss eines schriftlichen Vertrages Ausweiskopien seiner Kunden ein, die er anschließend aufbewahrte. Hierzu wählte er als datenschutzrechtliche Rechtsgrundlage die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO). Kunden konnten nur im Rahmen eines Opt-out-Verfahrens die Speicherung nachträglich schriftlich widerrufen.

Diese Vorgehensweise wurde von der rumänischen Datenschutzbehörde gerügt und das Unternehmen mit einem Bußgeld belegt sowie aufgefordert, die unrechtmäßig erhobenen Ausweiskopien zu löschen. Der Telekommunikationsanbieter bekämpfte die Entscheidung vor dem Landesgericht, das dann die Frage aufwarf, ob diese Vorgehensweise des Opt-outs (nach einem vorausgefüllten Häkchen im Vertrag) den Voraussetzungen der freiwilligen, informierten und aktiven Einwilligung entspreche. Die DSGVO verlangt für die Rechtmäßigkeit der Datenverarbeitung die freiwillige**,** informierte**,** bestimmte und aktiv erteilte Einwilligung des Betroffenen.

Ein vorausgefülltes Häkchen in einer Vertragsklausel sowie die Anforderung eines nachträglichen schriftlichen Widerrufs genügen der freiwilligen und aktiven Einwilligung nicht, da sie die tatsächliche Kenntnisnahme des Kunden nicht garantiert und für Kunden unklar ist, ob der Widerruf vertragsrelevante Konsequenzen haben könnte.

Zudem ist eine mündliche Informationserteilung durch den Telekommunikationsanbieter unzureichend, da für die erteilte Einwilligung die Rechenschaftspflicht nicht ausreichend erfüllt werden kann. Der EuGH bestätigt somit die strengen Anforderungen an die Einwilligung und bleibt seiner bisherigen Linie nach dem Planet49-Urteil treu.

2. Die Kontrolle durch die Instanzgerichte

Nachdem die DSGVO schon seit mehr als zwei Jahren angewandt wird, ist es zu einer Vielzahl von Entscheidungen gekommen, die sowohl hohe Bußgelder als auch klärende Anordnungen an Verantwortliche beinhalteten.

Die meisten Entscheidungen betrafen drei DSGVO-Schwerpunktverstöße[8]:

- Falsche oder unzureichende Wahl der Rechtsgrundlage der Datenverarbeitung (Art. 6, 9 bzw. 10 DSGVO)

[6] *EDPB*, Recommendations 01/2020, Rn. 68.
[7] EuGH 11. November 2020, C-61/19 – Orange Romania.
[8] https://www.enforcementtracker.com/?insights

- Unzureichende technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit
  (Art. 32 DSGVO)
- Nichteinhaltung der Grundsätze der Datenverarbeitung
  (Art. 5 DSGVO)

Entscheidungen von Datenschutzbehörden und Gerichten können im Instanzenzug bekämpft werden, wenn die unterlegene oder bestrafte Partei der Ansicht ist, in ihren Rechten verletzt worden zu sein.

In Österreich besteht gegen Erkenntnisse der Datenschutzbehörde das Rechtsmittel der Beschwerde vor dem Bundesverwaltungsgericht (BVwG). Bei Schadenersatzansprüchen richtet sich der Instanzenzug an das zuständige Oberlandesgericht (OLG).

Entscheidungen können dabei bestätigt, abgeändert oder Verfahren sogar gänzlich eingestellt werden.

Das 18 Mio EUR Straferkenntnis[9] der DSB gegen die Post AG wurde durch das Bundesverwaltungsgericht[10] vollständig behoben.

Hintergrund der erfolgreichen Beschwerde war die Tatsache, dass es der Datenschutzbehörde nicht gelungen ist, eine **natürliche Person** zu benennen, der das vorgeworfene rechtswidrige und schuldhafte Verhalten zugerechnet werden kann. Dies ist aber erforderlich, damit die Post AG als **juristische Person** bestraft werden kann.

Das österreichische Verwaltungsstrafrecht kennt keine Haftung juristischer Personen ohne Zurechnung eines rechtswidrigen Verhaltens natürlicher Personen. Unternehmen können nur dann für ein Fehlverhalten ihrer Mitarbeiter, Führungskräfte oder Geschäftsführung haften, wenn dieses auch zurechenbar ist.

Schon in einem früheren Verwaltungsstrafverfahren war es der DSB nicht gelungen, einen ausreichenden Anknüpfungspunkt für rechtswidriges Verhalten einer natürlichen Person zu ermitteln (siehe VwGH 12.05.2020 Ro 2019/04/0229).

Auch in Deutschland wurde eine Millionenstrafe gegen den Telekommunikationsanbieter 1&1 durch das Landesgericht Bonn[11] beträchtlich reduziert. Das Bußgeld iHv EUR 9,55 Mio wurde in der Instanz auf EUR 900.000 heruntergesetzt. Der vorgeworfene Verstoß betraf im Wesentlichen mangelhafte Datensicherheitsmaßnahmen bei der Authentifizierung von Betroffenen. Zur Bestätigung der Identität von 1&1-Kunden wurden nur deren Namen und Geburtsdatum abgefragt; anschließend stand ihnen der Zugriff auf alle anderen hinterlegten Daten offen.

Aufgrund dieser schwachen Authentifizierungsmaßnahmen wurden Daten eines Betroffenen an eine dritte Person weitergegeben und es kam zu Stalking. Obwohl es sich dabei um einen Einzelfall handelte, lagen doch im Wesentlichen strukturelle Mängel der Datensicherheit vor, die eine Vielzahl von Kunden betrafen. Die Höhe des Bußgeldes wurde im Rechtsmittelverfahren daher lediglich reduziert und nicht aufgehoben.

[9] DSB, 23.10.2019, DSB-D550.148/0017-DSB/2019.

[10] BVwG, 26.11.2020, W258 2227269-1/14E.

[11] LG Bonn v. 11.11.2020 Az. 29 OWi 1/20.

3. Internationale Erkenntnisse

Datenschutz

Die französische Datenschutzbehörde **CNIL** hat die Carrefour-Gruppe mit zwei Geldbußen iHv EUR 2,25 Mio und EUR 800.000 belegt.

Nach Eingang mehrerer Beschwerden hat die CNIL Verstöße gegen die DSGVO u.a. in Bezug auf die Erfüllung der Informationspflichten und die Wahrung von Betroffenenrechten festgestellt.

Demnach kam Carrefour Löschbegehren nicht nach und beschickte Betroffene trotz deren Widerruf weiterhin mit Direktmarketing bzw. nahm Widerrufe gar nicht erst entgegen.

Carrefour hatte auch ungerechtfertigt Identitätsnachweise verlangt, wenn Kunden ihre Betroffenenrechte ausüben wollten und speicherte die Daten von Kunden, die bereits seit fünf bis zehn Jahren keinerlei Geschäftsbeziehung mehr mit Carrefour unterhielten.

Cookies – E-Privacy-Bußgelder

Auch im Bereich des Telekommunikationsrechts wurde die CNIL tätig. Für den unrechtmäßigen Einsatz von Cookies wurden Millionenstrafen gegen die Branchenriesen Amazon und Google verhängt: Insgesamt EUR 100 Mio gegen Google (Google LLC und Google Ireland Ltd.) sowie EUR 35 Mio gegen Amazon.

Die Verstöße umfassen den Einsatz von Cookies ohne Einwilligung, intransparente Informationserteilung, fehlerhafte Cookie-Banner und mangelhafte Opt-in-Mechanismen.

Anders als in Österreich ist der Einsatz von Cookies in Frankreich auch im Datenschutzgesetz verankert, sodass hier die Datenschutzbehörde Bußgelder für Verstöße erteilen darf.

Irische Behörde wird tätig: Strafe gegen Twitter

Die vielkritisierte irische Datenschutzbehörde **DPC** ist zum ersten Mal seit DSGVO-Geltung gegen einen in Irland ansässigen US-Konzern tätig geworden.

Der Kurznachrichten-Dienst Twitter verabsäumte die umgehende Meldung eines Data Breach in der Zeit zwischen Weihnachten und Neujahr 2018/2019. Aufgrund eines internen Softwarefehlers wurden private Tweets der Öffentlichkeit zur Verfügung gestellt, ohne dass daraufhin die betroffenen Nutzer oder die zuständige Datenschutzbehörde verständigt wurden. Das erste irische Bußgeld gegen einen US-Konzern beläuft sich auf ca. EUR 450.000.

EDSA-Streitbeilegungsverfahren zwischen den EU-Aufsichtsbehörden

Diese Entscheidung ist vor allem insoweit interessant, als die irische Behörde zunächst ein wesentlich niedrigeres Bußgeld avisiert hatte. Dies führte jedoch zum Einspruch mehrerer europäischer Aufsichtsbehörden, vertreten durch die Hamburger Aufsichtsbehörde, die ein Streitbeilegungsverfahren gem. Art. 65 Abs. 1 lit. a DSGVO vor dem Europäischen Datenschutzausschuss geführt hat und darin die irische Behörde anwies[12], das Bußgeld entsprechend zu erhöhen.

Polnische Behörde straft Virgin Mobile

Wegen der fehlenden Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen wurde der Telekommunikationsanbieter Virgin Mobile Poland mit einem Bußgeld iHv ca. EUR 420.000 belegt. Im Zuge einer amtswegigen Prüfung wurde festgestellt, dass eine Überprüfung der technischen und organisatorischen Maßnahmen nur beiläufig erfolgte und

[12] Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR.

nicht alle Systeme umfasste, mit denen die Daten verarbeitet werden. Weiters wurde eine Schwachstelle im Zusammenhang mit dem Datenaustausch von Kundendaten mit Bezahldiensten festgestellt, die von einer unbefugten Person ausgenutzt wurde.

EUR 5 Mio Strafe gegen spanische Bank

Die spanische Datenschutzbehörde **AEPD** hat die Bank Banco Bilbao Vizcaya Argentaria, SA („BBVA“) wegen Verstößen gegen die Informationspflichten gem. Art. 13 DSGVO zu einem Bußgeld von EUR 5 Mio verurteilt.

Beanstandet wurden insbesondere Intransparenz, ungenaue Terminologien und Unklarheit in Bezug auf die verarbeiteten Daten. Die Datenverarbeitung war daher unrechtmäßig. Es wurden keine gültigen Einwilligungen eingeholt oder Opt-in-Mechanismen eingeführt.

4. Brexit

Am 31. Dezember 2020 um 23:00 Uhr endet der Übergangszeitraum und der Brexit tritt mit 1. Jänner 2021 in Kraft. Statt der EU-DSGVO gilt dann in Großbritannien die „UK-GDPR“, die im Wesentlichen die gleichen Grundsätze und Regelungen wie die bisherige DSGVO enthält, allerdings national beschränkt bleibt. Der bisherige Data Protection Act sowie die Privacy and Electronic Communications Regulations (PECR) bleiben in Geltung.

Ein Angemessenheitsbeschluss der Kommission über die Datenübermittlung an ein Nicht-EU-Land steht jedoch aus. Daher sind Datenübermittlungen in das Vereinte Königreich wie jene in Drittländer zu behandeln und entsprechende Standardvertragsklauseln abzuschließen.

Für die Datenübermittlung aus Großbritannien in die EU ändert sich nichts, da hier die DSGVO territorial und sachlich anwendbar bleibt.

5. Datenschutz- und Informationssicherheits-Zertifizierungen

Jedes Unternehmen ist zur Einhaltung der Datenschutzstandards verpflichtet. Dabei kann es einen erheblichen Wettbewerbsvorteil darstellen, wenn man seine Datenanwendungen oder Prozesse zertifizieren lässt.

Die wichtigsten Zertifizierungen in diesem Zusammenhang betreffen Normen der ISO-Reihe. Relevant sind dabei insbesondere die Normen zu Informationssicherheit-Managementsystemen (ISO/IEC 27001) und dokumentierten Qualitätsmanagementsystemen (ISO 9001).

Aber auch im Datenschutz kommt langsam Bewegung in die internationalen Zertifizierungen: Das Europäische Gütesiegel (European Privacy Seal – EuroPriSe) ist nunmehr einen Schritt weiter bei der Zulassung zu einem internationalen DSGVO-Zertifikat iSd Art. 42ff DSGVO.

Secur-Data hat dieses Jahr die Rezertifizierung eines IT-basierten Services betreut und der Verantwortliche konnte erneut erfolgreich mit dem EuroPriSe-Gütesiegel zertifiziert werden.

6. Seminarankündigung 2021

Wir freuen uns, Ihnen auch im nächsten Jahr mit unseren DSGVO-Praxisseminaren zur Verfügung zu stehen. Wir sind bemüht, einen Termin Ende März bzw. Mitte April für Sie ankündigen zu können. Falls Sie ein Inhouse-Seminar wünschen, können Sie uns jederzeit kontaktieren.

••••

Data Breach Konzept

Auswertungen der international verhängten Bußgelder zeigen, dass Verstöße gegen die sog. technischen und organisatorischen Sicherheitsmaßnahmen (TOMs) gem. Art. 32 DSGVO am schärfsten sanktioniert werden.

Menschliches Fehlverhalten ist eine der größten Risikoquellen in Unternehmen. Fehlende Sensibilisierung oder Unachtsamkeit können zu sogenannten Data Breaches (Datenschutzverletzungen) führen und nicht nur hohe Kosten, sondern auch Sanktionen durch Datenschutzbehörden und Gerichte nach sich ziehen. Dazu kommt, dass eine Datenschutzverletzung auch immensen Reputationsschaden mit sich bringen kann und damit in der Lage ist, das Unternehmen nachhaltig zu schädigen.

Wir unterstützen Sie bei der Ausarbeitung und Implementierung von **Richtlinien** für Mitarbeiter. Diese bilden gemeinsam mit **Dienstanweisungen** und **Betriebsvereinbarungen** das formale Konzept der organisatorischen Maßnahmen. Zudem bieten wir Ihnen technische Maßnahmen, um Ihr Unternehmen vor Datenschutzverletzungen zu schützen und deren Folgen zu bekämpfen. Hierbei kommen **Security Scans, Penetration Tests** und die **technische Überprüfung** bestehender Prozesse zur Anwendung.

Darüber hinaus bieten wir **Planspiele** für das **Incident-Response Management** an, um Mitarbeiterinnen und Mitarbeiter für den Ernstfall vorzubereiten und die richtigen Schlüsse aus einer Datenschutzverletzung zu ziehen.

Unsere Experten beraten Sie zu den Themen **Krisenmanagement** und **Krisenkommunikation** und schulen Datenschutzbeauftragte und -koordinatoren in Ihrem Unternehmen. Für eine unverbindliche Beratung können Sie uns unter office@secur-data.at kontaktieren oder unsere Website www.secur-data.at besuchen.

••••

Das Team der Secur-Data wünscht Ihnen frohe Weihnachten und ein gutes neues Jahr!